1996

The Quantitative Structure of Exponential Time

Jack H. Lutz

The Quantitative Structure of Exponential Time

Abstract
Department of Computer Science Iowa State University Ames, Iowa 50010 Recent results on the internal, measure-theoretic structure of the exponential time complexity classes linear polynomial E = DTIME(2) and E = DTIME(2) 2 are surveyed. The measure structure of these classes is seen to interact in informative ways with bi-immunity, complexity cores, polynomial-time many-one reducibility, circuit-size complexity, Kolmogorov complexity, and the density of hard languages. Possible implications for the structure of NP are also discussed.

Disciplines
Theory and Algorithms

The Quantitative Structure of Exponential Time

Jack H. Lutz [1]

ABSTRACT Recent results on the internal, measure-theoretic structure of the exponential time complexity classes E and EXP are surveyed. The measure structure of these classes is seen to interact in informative ways with bi-immunity, complexity cores, polynomial-time reductions, completeness, circuit-size complexity, Kolmogorov complexity, natural proofs, pseudorandom generators, the density of hard languages, randomized complexity, and lowness. Possible implications for the structure of NP are also discussed.

1 Introduction

In the past five years, new developments in resource-bounded measure have opened the way for a systematic investigation of the internal, measure-theoretic structure of the exponential time complexity classes E and EXP. The investigation is very far from complete, but it has already yielded a number of interesting insights and results. This paper surveys the motivations, ideas, and results of the earliest phase of the investigation, i.e., the part completed by mid-1995.

It should be emphasized that the material surveyed here is the work of several investigators. The ongoing efforts of these investigators, together with the efforts of more recent participants, virtually guarantee that this survey will be incomplete by the time it appears. (At the time of this writing, there are already several papers in review and manuscripts in circulation that appear to extend the body of knowledge presented here.) Nevertheless, it is to be hoped that the "organized snapshot" provided by this survey will provide context and motivation for future research.

There are three reasons for our interest in the complexity classes E and EXP.

(i) E and EXP have rich, apparently well-behaved, internal structures. These structures have many interacting facets, including a variety of

[1]Department of Computer Science, Iowa State University, Ames, IA 50011. E-mail: lutz@cs.iastate.edu. This research was supported in part by National Science Foundation Grant CCR-9157382, with matching funds from Rockwell International, Microware Systems Corporation, and Amoco Foundation.

reducibilities [LLS75], complete languages under these reducibilities [SC79, Wat87b], measure structure [Lut92], and category structure [Lut90, Fen91, Fen95].

(ii) EXP is the smallest deterministic time complexity class known to contain NP. It also contains PSPACE, and hence the polynomial-time hierarchy and many other classes of interest in complexity theory. E is a proper subset of EXP, but it contains P and "the essential part of NP" [Wat87b], i.e., many NP-complete problems.

(iii) E and EXP have been proven to contain intractable problems [HS65]. From the standpoint of complexity theory, this existence of intractability is a valuable resource. This is because, in practice, a proof that a specific language A is intractable proceeds by *inferring* the intractability of A from the intractability of some language B chosen or constructed for this purpose.

Taken together, (i), (ii), and (iii) suggest E and EXP as appropriate *spaces* in which to investigate (embed) problems involving NP, PH, PSPACE, and other classes in this range.

Until recently, the issues addressed by research on the structure of complexity classes have been largely qualitative rather than quantitative. (Indeed, the introduction to [Sch86b] offered "qualitative" as a synonym for "structural.") This seemed to be an inevitable aspect of the subject. A problem is, or is not, complete for a complexity class. One complexity class is, or is not, contained in another. This was unfortunate, since the objective of complexity theory is a quantitative theory of computation. However, since the sets of interest are all countably infinite, there appeared to be no possibility of making quantitative versions of these judgments.

The main objective of the work surveyed here is to remedy this situation.

Suppose that a language $A \subseteq \{0,1\}^*$ is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether each string is in A. Then *classical* Lebesgue measure theory (described in [Hal50, Oxt80], for example) identifies certain *measurable sets* of languages (also called *events*) and assigns to each measurable set X a *measure* $\mu(X)$, which is the probability that $A \in X$ in this experiment. A set X of languages is then small in the sense of measure if it has measure 0. *Effective* measure theory, which says what it means for a set of decidable languages to have measure 0 as a subset of the set of all such languages, has been investigated by Freidzon [Fre72], Mehlhorn [Meh74], and others. The *resource-bounded* measure theory introduced by Lutz [Lut92, Lutb] has the classical and effective theories as special cases, but also defines measurability and measure for subsets of many complexity classes. The *small* subsets of such a complexity class are then the measure 0 sets; the *large* subsets are the measure 1 sets (complements of measure 0 sets). We say that *almost*

every language in a complexity class $\mathcal{C}$ has a given property if the set of languages in $\mathcal{C}$ exhibiting the property is a measure 1 subset of $\mathcal{C}$.

Thus, resource-bounded measure provides a means of investigating the *sizes* of various subsets of E and EXP. This is *a priori* a hopeful development, both because quantitative results are more informative and because Lebesgue measure has been so useful in analysis, probability, and mathematical physics. However, much of the ongoing motivation for this work arises not from *a priori* considerations, but rather from the fact that resource-bounded measure turns out to interact informatively with many properties of interest in computational complexity. Such interactions surveyed in this paper involve bi-immunity (section 4), complexity cores (sections 5, 7, and 8), the structure of E and EXP under polynomial-time reductions (sections 6,7, and 8), circuit-size complexity and time-bounded Kolmogorov complexity (section 9), natural proofs and pseudorandom generators (section 9), the density of hard languages (section 11), and other properties that had been extensively studied prior to the advent of resource-bounded measure. It is to be hoped that sustained, systematic investigation along these lines will lead to a detailed, quantitative understanding of E and EXP.

From the standpoint of classical mathematics and recursion theory, classes like P, NP, PH, and PSPACE are all negligibly small, hence difficult to distinguish by quantitative structural means. From the standpoint of E and EXP, matters may be very different. If EXP is, indeed, the smallest deterministic time class containing NP, then there may well be a natural "notion of smallness" for subsets of EXP such that P is a small subset of EXP, but NP is not. Similarly, it may be that P is a small subset of E, but that $\mathrm{NP} \cap \mathrm{E}$ is not.

It is possible that resource-bounded measure already provides such a notion of smallness. It is certainly the case that P has measure 0 in E and EXP [Lut92]. In section 12 we discuss the reasonableness and known consequences of the hypothesis that NP is not small in this sense. This is a very strong hypothesis that appears to have much more explanatory power than traditional, qualitative hypotheses, such as $\mathrm{P} \neq \mathrm{NP}$ or the separation of the polynomial-time hierarchy. Only further investigation will determine whether this hypothesis is reasonable.

2 Preliminaries

In this paper, $[\![\psi]\!]$ denotes the *Boolean value* of the condition ψ, i.e., $[\![\psi]\!] =$ if ψ then 1 else 0.

All *languages* here are sets of binary strings, i.e., sets $A \subseteq \{0,1\}^*$. We identify each language A with its *characteristic sequence* $\chi_A \in \{0,1\}^\infty$

defined by

$$\chi_A = [\![s_0 \in A]\!][\![s_1 \in A]\!][\![s_2 \in A]\!]...,$$

where $s_0 = \lambda$, $s_1 = 0$, $s_2 = 1$, $s_3 = 00, ...$ is the standard enumeration of $\{0,1\}^*$. Relying on this identification, the set $\{0,1\}^\infty$, consisting of all infinite binary sequences, will be regarded as the set of all languages.

We say that a condition $\theta(n)$ holds *almost everywhere* (*a.e.*) if it holds for all but finitely many $n \in \mathbf{N}$. We say that $\theta(n)$ holds *infinitely often* (*i.o.*) if it holds for infinitely many $n \in \mathbf{N}$.

For $A \subseteq \{0,1\}^*$ and $n \in \mathbf{N}$, we use the notations $A_{=n} = A \cap \{0,1\}^n$ and $A_{\leq n} = A \cap \{0,1\}^{\leq n}$. A language A is *sparse* if there is a polynomial $q(n)$ such that $|A_{\leq n}| \leq q(n)$ a.e. A language A is *dense* if there is a real number $\varepsilon > 0$ such that $|A_{\leq n}| > 2^{n^\varepsilon}$ a.e.

The *symmetric difference* of languages A and B is $A \triangle B = (A - B) \cup (B - A)$. The *complement* of a language $A \subseteq \{0,1\}^*$ is $A^c = \{0,1\}^* - A$. The *complement* of a set X of languages is $X^c = \{\, A \subseteq \{0,1\}^* \mid A \notin X \,\}$.

We fix a one-to-one pairing function $\langle , \rangle$ from $\{0,1\}^* \times \{0,1\}^*$ onto $\{0,1\}^*$ such that the pairing function and its associated projections, $\langle x, y\rangle \mapsto x$ and $\langle x, y\rangle \mapsto y$, are computable in polynomial time.

For a function $f : \{0,1\}^* \to \{0,1\}^*$ and a natural number i, we define the function $f_i : \{0,1\}^* \to \{0,1\}^*$ by $f_i(x) = f(\langle 0^i, x\rangle)$. We then regard f as a "uniform enumeration" of the functions $f_0, f_1, f_2, \cdots$.

In general, complexity classes of functions from $\{0,1\}^*$ into $\{0,1\}^*$ will be denoted by appending an 'F' to the notation for the corresponding complexity classes of languages. Thus, for $t : \mathbf{N} \to \mathbf{N}$, DTIMEF($t$) is the set of all functions $f : \{0,1\}^* \to \{0,1\}^*$ such that $f(x)$ is computable in $O(t(|x|))$ time.

3 Resource-bounded measure

In this section we introduce a fragment of resource-bounded measure that is sufficient for understanding the meaning of the results surveyed in this paper. Although resource-bounded measure is a very general theory whose special cases include classical Lebesgue measure, the measure structure of the class REC of all recursive languages, and measure in various complexity classes, our discussion here will be specific to the classes E and E_2. The interested reader is referred to [Lut92, Lutb, May94b, Jue94, JL95b, ATZ] for more discussion, examples, and technical machinery.

Definition. A *martingale* is a function $d : \{0,1\}^* \to [0, \infty)$ with the property that, for all $w \in \{0,1\}^*$,

$$d(w) = \frac{d(w0) + d(w1)}{2}. \qquad (*)$$

A martingale d *succeeds* on a language $A \subseteq \{0,1\}^*$ if

$$\limsup_{n\to\infty} d(\chi_A[0..n-1]) = \infty.$$

Intuitively, a martingale d is a betting strategy that, given a language A, starts with capital (amount of money) $d(\lambda)$ and bets on the membership or nonmembership of the successive strings $s_0, s_1, s_2, \cdots$ (the standard enumeration of $\{0,1\}^*$) in A. Prior to betting on a string s_n, the strategy has capital $d(w)$, where $w = [\![s_0 \in A]\!] \cdots [\![s_{n-1} \in A]\!]$. After betting on the string s_n, the strategy has capital $d(wb)$, where $b = [\![s_n \in A]\!]$. Condition $(*)$ ensures that the betting is fair. The strategy succeeds on A if its capital is unbounded as the betting progresses.

Martingales were used extensively by Schnorr [Sch70, Sch71a, Sch71b, Sch73] in his investigation of random and pseudorandom sequences. Here we use martingales as a way to define measure 0 sets.

Consider the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in A. Given a set X of languages, let $\Pr(X) = \mathrm{Prob}_A[A \in X]$ denote the probability that $A \in X$ when A is chosen in this fashion. (If X is not Lebesgue measurable, then $\Pr(X)$ will not exist, but this issue can be safely ignored here.) The following fact is intuitively clear and not difficult to prove.

Proposition 3.1. For every set X of languages, the following two conditions are equivalent.

(1) $\Pr(X) = 0$.

(2) There is a martingale d such that d succeeds on every element of X.

In order to generalize Proposition 3.1 we need to consider martingales that are computable within some resource bound. Since martingales are real-valued, their computations must employ finite approximations of real numbers. For this purpose, we consider functions of the form $d : \mathbf{N}^k \times \{0,1\}^* \to \mathbf{Q}$, where $\mathbf{Q}$ is the set of rational numbers. Formally, in order to have uniform criteria for computational complexity, we consider all such functions to map $\{0,1\}^*$ to $\{0,1\}^*$. For example, a function $d : \mathbf{N} \times \{0,1\}^* \to \mathbf{Q}$ is formally interpreted as a function $\tilde{d} : \{0,1\}^* \to \{0,1\}^*$. Under this interpretation, $d(r,w) = q$ means that $\tilde{d}(\langle 0^r, w\rangle) = \langle u, v\rangle$, where u and v are the binary representations of the numerator and denominator of q, respectively. We also write $d_r(w)$ for $d(r,w)$.

Definition. The classes $\mathrm{p}_1 = \mathrm{p}$ and p_2, both consisting of functions $f : \{0,1\}^* \to \{0,1\}^*$, are defined as follows.

$$\begin{aligned} \mathrm{p}_1 &= \{f \mid f \text{ is computable in polynomial time}\} \\ \mathrm{p}_2 &= \{f \mid f \text{ is computable in } n^{(\log n)^{O(1)}} \text{ time}\} \end{aligned}$$

Guided by Proposition 3.1, the measure structures of E and EXP are now developed in terms of the classes p_i, for $i = 1, 2$.

Definition. A martingale d is p_i-*computable* if there is a function $\widehat{d} : \mathbf{N} \times \{0,1\}^* \to \mathbf{Q}$ such that $\widehat{d} \in \mathrm{p}_i$ and, for all $r \in \mathbf{N}$ and $w \in \{0,1\}^*$,

$$\left| \widehat{d}_r(w) - d(w) \right| \leq 2^{-r}.$$

A p_i-*martingale* is a martingale that is p_i-computable.

We now come to the key idea of this section.

Definition. A set X of languages has p_i-*measure 0*, and we write $\mu_{\mathrm{p}_i}(X) = 0$, if there is a p_i-martingale d that succeeds on every element of X. A set X of languages has p_i-measure 1, and we write $\mu_{\mathrm{p}_i}(X) = 1$, if $\mu_{\mathrm{p}_i}(X^c) = 0$.

We now turn to the internal measure structures of the classes $\mathrm{E}_1 = \mathrm{E}$ and $\mathrm{E}_2 = \mathrm{EXP}$. [1]

Definition. A set X has *measure 0 in* E_i, and we write $\mu(X \mid \mathrm{E}_i) = 0$, if $\mu_{\mathrm{p}_i}(X \cap \mathrm{E}_i) = 0$. A set X has *measure 1 in* E_i, and we write $\mu(X \mid \mathrm{E}_i) = 1$, if $\mu(X^c \mid \mathrm{E}_i) = 0$. If $\mu(X \mid \mathrm{E}_i) = 1$, we say that *almost every* language in E_i is in X.

We write $\mu(X \mid \mathrm{E}_i) \neq 0$ to indicate that X does *not* have measure 0 in E_i. Note that this does *not* assert that "$\mu(X \mid \mathrm{E}_i)$" has some nonzero value.

The following is obvious but useful.

Fact 3.2. For every set $X \subseteq \{0,1\}^\infty$,

$$\begin{array}{ccccc} \mu_{\mathrm{p}}(X) = 0 & \Longrightarrow & \mu_{\mathrm{p}_2}(X) = 0 & \Longrightarrow & \Pr[A \in X] = 0 \\ \Downarrow & & \Downarrow & & \\ \mu(X \mid \mathrm{E}) = 0 & & \mu(X \mid \mathrm{EXP}) = 0, & & \end{array}$$

where the probability $\Pr[A \in X]$ is computed according to the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen probabilistically,

---

[1] The classes E and EXP are the first two classes in a natural hierarchy $\mathrm{E}_1, \mathrm{E}_2, \mathrm{E}_3, \ldots$ of exponential time complexity classes. In [Lut92], the measure structures of these classes are developed in terms of a corresponding hierarchy $\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3, \ldots$ of function classes. Consequently, most papers on resource-bounded measure (including all of the author's papers) use the notation E_2 in place of EXP. However, in this book, for the sake of consistency, we refrain from using the E_i notation. The only exceptions are the present section and a brief mention of the class E_3 in section 9.

using an independent toss of a fair coin to decide whether each string $x \in \{0,1\}^*$ is in A.

It is shown in [Lut92] that these definitions endow E and EXP with internal measure structure. This structure justifies the intuition that, if $\mu(X \mid \mathrm{E}) = 0$, then $X \cap \mathrm{E}$ is a *negligibly small* subset of E (and similarly for EXP). The most important component of this justification is the Measure Conservation Theorem [Lut92], which implies the following.

Theorem 3.3 (Lutz [Lut92]). $\mu(\mathrm{E}|\mathrm{E}) \neq 0$ and $\mu(\mathrm{EXP}|\mathrm{EXP}) \neq 0$.

The following result shows that, if $\mathcal{C}$ is a "reasonable" complexity class that contains almost every element of E (respectively, EXP), then $\mathcal{C}$ contains *every* element of E (respectively, EXP).

Theorem 3.4 (Regan, Sivakumar, and Cai [RSC95]). Let $\mathcal{C}$ be a set of languages that is either closed under symmetric difference or closed under (finite) union and intersection.

1. If $\mu(\mathcal{C}|\mathrm{E}) = 1$, then $\mathrm{E} \subseteq \mathcal{C}$.
2. If $\mu(\mathcal{C}|\mathrm{EXP}) = 1$, then $\mathrm{EXP} \subseteq \mathcal{C}$.

Resource-bounded measure in E and EXP is known to be robust with respect to various changes in the definition [Lut92, Lutb, May94b, JL95b]. Recently, Buhrman and Longpré [BL96] have shown that resource-bounded measure can also be characterized in terms of the compressibility (and decompressibility) of languages.

4 Incompressibility and bi-immunity

Many results on the structure of E and EXP under $\leq_m^{\mathrm{P}}$-reducibility use languages that are "incompressible by many-one reductions." This idea, originally exploited by Meyer [Mey77], is developed in the following definitions.

Definition. The *collision set* of a function $f : \{0,1\}^* \to \{0,1\}^*$ is

$$C_f = \{x \in \{0,1\}^* \mid (\exists y < x) f(y) = f(x)\}.$$

Here, we are using the standard ordering $s_0 < s_1 < s_2 < \cdots$ of $\{0,1\}^*$.

Note that f is one-to-one if and only if $C_f = \emptyset$.

Definition. A function $f : \{0,1\}^* \to \{0,1\}^*$ is *one-to-one almost everywhere* (or, briefly, *one-to-one a.e.*) if its collision set C_f is finite.

Definition. Let $A, B \subseteq \{0,1\}^*$ and let $t : \mathbf{N} \to \mathbf{N}$. A $\leq_m^{\mathrm{DTIME}(t)}$-*reduction of A to B* is a function $f \in \mathrm{DTIMEF}(t)$ such that $A = f^{-1}(B)$, i.e., such that, for all $x \in \{0,1\}^*$, $x \in A$ iff $f(x) \in B$. A $\leq_m^{\mathrm{DTIME}(t)}$-*reduction of A* is a function f that is a $\leq_m^{\mathrm{DTIME}(t)}$-reduction of A to $f(A)$.

It is easy to see that f is a $\leq_m^{\mathrm{DTIME}(t)}$-reduction of A if and only if there exists a language B such that f is a $\leq_m^{\mathrm{DTIME}(t)}$-reduction of A to B.

Definition. Let $t : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is *incompressible by $\leq_m^{\mathrm{DTIME}(t)}$-reductions* if every $\leq_m^{\mathrm{DTIME}(t)}$-reduction of A is one-to-one a.e. A language $A \subseteq \{0,1\}^*$ is *incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions* if it is incompressible by $\leq_m^{\mathrm{DTIME}(q)}$-reductions for all polynomials q.

Intuitively, if f is a $\leq_m^{\mathrm{DTIME}(t)}$-reduction of A to B and C_f is large, then f compresses many questions "$x \in A$?" to fewer questions "$f(x) \in B$?" If A is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions, then very little such compression can occur.

Meyer [Mey77] proved that E contains languages that are incompressible by $\leq_m^{\mathrm{P}}$-reductions. The following result shows that almost every language in E has this property.

Theorem 4.1 (Juedes and Lutz [JL95a]). Let $c \in \mathbf{Z}^+$ and define the sets

$$X = \{A \subseteq \{0,1\}^* | A \text{ is incompressible by } \leq_m^{\mathrm{DTIME}(2^{cn})}\text{-reductions}\},$$

$$Y = \{A \subseteq \{0,1\}^* | A \text{ is incompressible by } \leq_m^{\mathrm{DTIME}(2^{n^c})}\text{-reductions}\}.$$

Then $\mu_{\mathrm{p}}(X) = \mu_{\mathrm{p}_2}(Y) = 1$. Thus almost every language in E is incompressible by $\leq_m^{\mathrm{DTIME}(2^{cn})}$-reductions, and almost every language in EXP is incompressible by $\leq_m^{\mathrm{DTIME}(2^{n^c})}$-reductions.

Sketch of proof that $\mu_{\mathrm{p}}(X) = 1$. It suffices to exhibit a p-martingale $d : \{0,1\}^* \to [0,\infty)$ that succeeds on every element of X^c.

Let $f \in \mathrm{DTIMEF}(2^{(c+1)n})$ be universal for $\mathrm{DTIMEF}(2^{cn})$, in the sense that $\mathrm{DTIMEF}(2^{cn}) = \{f_i | i \in \mathbf{N}\}$. For each $i \in \mathbf{N}$, define a set Z_i of languages as follows. If the collision set C_{f_i} is finite, then $Z_i = \emptyset$. Otherwise, if C_{f_i} is infinite, then Z_i is the set of all languages A such that f_i is a $\leq_m^{\mathrm{DTIME}(2^{cn})}$-reduction of A. Note that X^c is the union of the sets Z_i. The martingale d is defined by

$$d(w) = \sum_{i=0}^{\infty} 2^{-i} d_i(w),$$

where the functions $d_i : \{0,1\}^* \to [0,\infty)$ are defined as follows. Let $i \in \mathbf{N}$, $w \in \{0,1\}^*$, and $b \in \{0,1\}$. Recall that $s_0, s_1, s_2, \cdots$ is a standard enumeration of $\{0,1\}^*$.

(i) $d_i(\lambda) = 1$.

(ii) If $s_{|w|} \notin C_{f_i}$, then $d_i(wb) = d_i(w)$.

(iii) If $s_{|w|} \in C_{f_i}$, then fix the least $j \in \mathbf{N}$ such that $f_i(s_j) = f_i(s_{|w|})$ and set

$$d_i(wb) = 2 \cdot d_i(w) \cdot [\![b = w[j]]\!].$$

It is easy to check that each d_i is a martingale, whence d itself is a martingale. Intuitively, d_i bets on membership of strings in a language A. Clause (i) says that d_i starts with 1 dollar. Clause (ii) says that d_i does not bet on the status of strings $x \notin C_{f_i}$. Clause (iii) says that, for strings $x \in C_{f_i}$, d_i bets all its capital that $x \in A$ iff $y \in A$, where y is the first string such that $f_i(x) = f_i(y)$. If $A \in Z_i$, then this bet will be correct, thereby doubling d_i's capital, infinitely often. Thus d_i succeeds on every element of Z_i. It follows from this that d succeeds on every element of X^c.

Finally, to see that d is p-computable, define $\widehat{d} : \mathbf{N} \times \{0,1\}^* \to \mathbf{Q}$ by

$$\widehat{d}_r(w) = \sum_{i=0}^{r+|w|} 2^{-i} d_i(w).$$

Since $f \in \mathrm{DTIMEF}(2^{(c+1)n})$ and the computation of $d_i(w)$ only uses values $f_i(u)$ for strings u with $|u| = O(\log |w|)$, it is clear that $d \in \mathrm{p}$. Since

$$\left| \widehat{d}_r(w) - d(w) \right| = \sum_{i=r+|w|+1}^{\infty} 2^{-i} d_i(w) \leq \sum_{i=r+|w|+1}^{\infty} 2^{|w|-i} = 2^{-r}$$

for all $r \in \mathbf{N}$ and $w \in \{0,1\}^*$, it follows that d is p-computable. □

Corollary 4.2 (Juedes and Lutz [JL95a]). Almost every language in E and almost every language in EXP is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions.

Corollary 4.3 (Meyer [Mey77]). There is a language $A \in \mathrm{E}$ that is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions.

We conclude this section with a brief discussion of P-bi-immunity.

Definition. A language $A \subseteq \{0,1\}^*$ is P-*immune* if, for all languages $B \subseteq A$, $B \in \mathrm{P}$ implies that B is finite. A language $A \subseteq \{0,1\}^*$ is P-*bi-immune* if A and A^c are both P-immune.

Intuitively, a language that is P-bi-immune "cannot be nontrivially approximated, from inside or outside," by any language in P.

Proposition 4.4 (Ko and Moore [KM75]). Every language that is incompressible by $\leq^{\mathrm{P}}_{m}$-reductions is P-bi-immune.

In light of this proposition, languages that are incompressible by $\leq_m^{\mathrm{P}}$-reductions are sometimes called "strongly P-bi-immune" [BS85, BDG90].

The following result shows that almost every language in E is P-bi-immune.

Theorem 4.5 (Mayordomo [May94a]). Almost every language in E, and almost every language in EXP, is P-bi-immune.

Although Theorem 4.5 follows immediately from Corollary 4.2 and Proposition 4.4, it should be noted that Mayordomo's proof of this result preceded, and was independent of, the proofs of Theorem 4.1 and Corollary 4.2.

5 Complexity cores

Complexity cores, first introduced by Lynch [Lyn75], have been studied extensively. (See [BDG90] for an overview of such work.) Intuitively, a complexity core of a language A is a fixed set K of inputs such that *every* machine whose decisions are consistent with A fails to decide efficiently on all but finitely many elements of K. The meaning of "efficiently" is a parameter of the definition that varies according to the context. In this section we make this definition precise and note that almost every language in E and EXP has very large complexity cores.

Given a machine M and an input $x \in \{0,1\}^*$, we write $M(x) = 1$ if M accepts x, $M(x) = 0$ if M rejects x, and $M(x) = \perp$ in any other case (i.e., if M fails to halt or M halts without deciding x). If $M(x) \in \{0,1\}$, we write $time_M(x)$ for the number of steps used in the computation of $M(x)$. If $M(x) = \perp$, we define $time_M(x) = \infty$. We partially order the set $\{0, 1, \perp\}$ by $\perp < 0$ and $\perp < 1$, with 0 and 1 incomparable. A machine M is *consistent* with a language $A \subseteq \{0,1\}^*$ if $M(x) \leq [\![x \in A]\!]$ for all $x \in \{0,1\}^*$.

Definition. Let $t : \mathbf{N} \to \mathbf{N}$ be a time bound and let $A, K \subseteq \{0,1\}^*$. Then K is a DTIME($t(n)$)-*complexity core* of A if, for every $c \in \mathbf{N}$ and every machine M that is consistent with A, the "fast set"

$$F = \{x \,|\, time_M(x) \leq c \cdot t(|x|) + c\}$$

satisfies $|F \cap K| < \infty$. (By our definition of $time_M(x)$, $M(x) \in \{0,1\}$ for all $x \in F$. Thus F is the set of all strings that M "decides efficiently.")

Note that every subset of a DTIME($t(n)$)-complexity core of A is a DTIME($t(n)$)-complexity core of A. Note also that, if $s(n) = O(t(n))$, then every DTIME($t(n)$)-complexity core of A is a DTIME($s(n)$)-complexity core of A.

Definition. Let $A, K \subseteq \{0,1\}^*$.

1. K is a *polynomial complexity core* (or, briefly, a P-*complexity core*) of A if K is a DTIME(n^k)-complexity core of A for all $k \in \mathbf{N}$.

2. K is an *exponential complexity core* of A if there is a real number $\epsilon > 0$ such that K is a DTIME(2^{n^ϵ})-complexity core of A.

Intuitively, a P-complexity core of A is a set of infeasible instances of A, while an exponential complexity core of A is a set of extremely hard instances of A.

The following observation, an obvious generalization of a result of Balcázar and Schöning [BS85] (see Corollary 5.2 below), relates incompressibility to complexity cores.

Lemma 5.1 (Juedes and Lutz [JL95a]). If $t : \mathbf{N} \to \mathbf{N}$ is time constructible then every language that is incompressible by $\leq_m^{\mathrm{DTIME}(t)}$-reductions has $\{0,1\}^*$ as a DTIME(t)-complexity core.

Corollary 5.2. Let $c \in \mathbf{N}$.

1. (Balcázar and Schöning [BS85]) Every language that is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions has $\{0,1\}^*$ as a P-complexity core.

2. Every language that is incompressible by $\leq_m^{\mathrm{DTIME}(2^{cn})}$-reductions has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core.

3. Every language that is incompressible by $\leq_m^{\mathrm{DTIME}(2^{n^c})}$-reductions has $\{0,1\}^*$ as a DTIME(2^{n^c})-complexity core.

Theorem 4.1 and Corollary 5.2 now tell us that almost every language decidable in exponential time has complexity cores of the largest possible size.

Corollary 5.3 (Juedes and Lutz [JL95a]). Let $c \in \mathbf{Z}^+$.

1. Almost every language in E has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core.

2. Almost every language in EXP has $\{0,1\}^*$ as a DTIME(2^{n^c})-complexity core.

6 Small span theorems

In this section we describe research on small span theorems, which illuminate key aspects of the structure of E and EXP under polynomial reductions. We begin with the Small Span Theorem for $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions.

Define the *lower* $\leq_m^{\mathrm{P}}$-*span* of a language $A \subseteq \{0,1\}^*$ to be

$$\mathrm{P}_m(A) = \{B \subseteq \{0,1\}^* \mid B \leq_{\mathrm{m}}^{\mathrm{P}} A\}.$$

Similarly, define the *upper* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-span* of A to be

$$\mathrm{P}_m^{-1}(A) = \{B \subseteq \{0,1\}^* \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\}.$$

Intuitively, in the $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility structure of the set of all languages, we think of $\mathrm{P}_m(A)$ as lying "below" A, while $\mathrm{P}_m^{-1}(A)$ lies "above" A. (See Figure 1.) We will be especially concerned with the size, i.e., the resource-bounded measure, of the upper and lower spans of various languages. If neither of these spans is small (i.e., neither has resource-bounded measure 0), then we have the configuration depicted schematically in Figure 1. On the other hand, if one or both of these spans is small, then we have one of the "small-span" configurations depicted schematically in Figure 2. The Small $\leq_{\mathrm{m}}^{\mathrm{P}}$-Span Theorem says that, if A is in E or EXP, *then at least one of the sets* $\mathrm{P}_m(A)$, $\mathrm{P}_m^{-1}(A)$ *is small.* That is, only small-span configurations can occur in E or EXP.

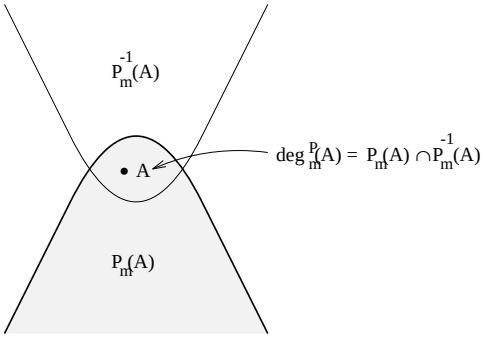

FIGURE 1. The upper span, lower span (shaded), and degree of A.

Theorem 6.1 (Small $\leq_{\mathrm{m}}^{\mathrm{P}}$-Span Theorem—Juedes and Lutz [JL95a]).

1. For every $A \in \mathrm{E}$,

$$\mu(\mathrm{P}_m(A) \mid \mathrm{E}) = 0$$

or

$$\mu_{\mathrm{p}}(\mathrm{P}_m^{-1}(A)) = \mu(\mathrm{P}_m^{-1}(A) \mid \mathrm{E}) = 0.$$

2. For every $A \in \mathrm{EXP}$,

$$\mu(\mathrm{P}_m(A) \mid \mathrm{EXP}) = 0$$

or

$$\mu_{\mathrm{p}_2}(\mathrm{P}_m^{-1}(A)) = \mu(\mathrm{P}_m^{-1}(A) \mid \mathrm{EXP}) = 0.$$

Ambos-Spies [Amb86] has shown that $\mathrm{P}_m{}^{-1}(A)$ has Lebesgue measure 0 whenever $A \notin \mathrm{P}$. The following lemma obtains a stronger conclusion (resource-bounded measure 0) from a stronger hypothesis on A.

Lemma 6.2 (Juedes and Lutz [JL95a]). Let A be a language that is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions.
1. If $A \in \mathrm{E}$, then $\mu_{\mathrm{p}}(\mathrm{P}_m^{-1}(A)) = 0$, and hence $\mu(\mathrm{P}_m^{-1}(A) \mid \mathrm{E}) = 0$.
2. If $A \in \mathrm{EXP}$, then $\mu_{\mathrm{p}_2}(\mathrm{P}_m^{-1}(A)) = 0$, and hence $\mu(\mathrm{P}_m^{-1}(A) \mid \mathrm{EXP}) = 0$.

We do not prove this lemma here, but we use it to prove the Small Span Theorem.

Proof of Theorem 6.1. To prove 1, let $A \in \mathrm{E}$ and let X be the set of all languages that are incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions. We have two cases.

Case I. If $\mathrm{P}_m(A) \cap \mathrm{E} \cap X = \emptyset$, then Corollary 4.2 tells us that $\mu(\mathrm{P}_m(A) \mid \mathrm{E}) = 0$.

Case II. If $\mathrm{P}_m(A) \cap \mathrm{E} \cap X \neq \emptyset$, then fix a language $B \in \mathrm{P}_m(A) \cap \mathrm{E} \cap X$. Since $B \in \mathrm{E} \cap X$, Lemma 6.2 tells us that

$$\mu_{\mathrm{p}}(\mathrm{P}_m^{-1}(B)) = \mu(\mathrm{P}_m^{-1}(B) \mid \mathrm{E}) = 0.$$

Since $\mathrm{P}_m^{-1}(A) \subseteq \mathrm{P}_m^{-1}(B)$, it follows that

$$\mu_{\mathrm{p}}(\mathrm{P}_m^{-1}(A)) = \mu(\mathrm{P}_m^{-1}(A) \mid \mathrm{E}) = 0.$$

This proves 1. The proof of 2 is identical. □

Using the Small Span Theorem, we note that $\leq^{\mathrm{P}}_m$-hard languages for E are extremely rare.

Theorem 6.3 (Juedes and Lutz [JL95a]). Let $\mathcal{H}_m(\mathrm{E})$ be the set of all languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E. Then $\mu_{\mathrm{p}}(\mathcal{H}_m(\mathrm{E})) = 0$.

Proof. Let A be as in Corollary 4.3. Then $\mathcal{H}_m(\mathrm{E}) \subseteq \mathrm{P}_m^{-1}(A)$, so Lemma 6.2 tells us that

$$\mu_{\mathrm{p}}(\mathcal{H}_m(\mathrm{E})) = \mu_{\mathrm{p}}(\mathrm{P}_m^{-1}(A)) = 0.$$

□

Recently, Ambos-Spies, Neis, and Terwijn [ANT] have used resource-bounded genericity to prove the extension of Lemma 6.2 obtained by substituting $\leq^{\mathrm{P}}_{k-\mathrm{tt}}$-reductions and $\mathrm{P}^{-1}_{\mathrm{k-tt}}(\mathrm{A})$ for $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions and $\mathrm{P}^{-1}_{\mathrm{m}}(\mathrm{A})$, respectively, where k is a fixed positive integer. From this they have obtained the following extension of Theorem 6.1.

Theorem 6.4 (Small $\leq^{\mathrm{P}}_{k-\mathrm{tt}}$-Span Theorem - Ambos-Spies, Neis, and Terwijn [ANT]). Let k be a positive integer.

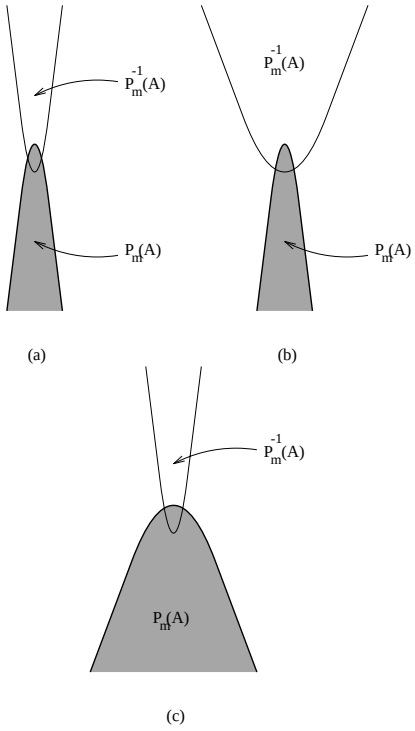

FIGURE 2. Small-span configurations. (Narrow regions depict measure 0 spans.)

1. For every $A \in \mathrm{E}$,
$$\mu(\mathrm{P}_{k-\mathrm{tt}}(A)|\mathrm{E}) = 0$$
or
$$\mu_{\mathrm{p}}(\mathrm{P}^{-1}_{\mathrm{k-tt}}(\mathrm{A})) = \mu(\mathrm{P}^{-1}_{\mathrm{k-tt}}(\mathrm{A})|\mathrm{E}) = 0$$
2. For every $A \in \mathrm{EXP}$,
$$\mu(\mathrm{P}_{\mathrm{k-tt}}(\mathrm{A})|\mathrm{EXP}) = 0$$
or
$$\mu_{\mathrm{p_2}}(\mathrm{P}^{-1}_{\mathrm{k-tt}}(\mathrm{A})) = \mu(\mathrm{P}^{-1}_{\mathrm{k-tt}}(\mathrm{A})|\mathrm{EXP}) = 0$$

This immediately yields the following extension of Theorem 6.3.

Theorem 6.5 (Ambos-Spies, Neis, and Terwijn [ANT]). Let k be a positive integer. If $\mathcal{H}_{k-\mathrm{tt}}(\mathrm{E})$ is the set of all languages that are $\leq^{\mathrm{P}}_{k-\mathrm{tt}}$-hard for E, then $\mu_{\mathrm{p}}(\mathcal{H}_{k-\mathrm{tt}}(\mathrm{E})) = 0$.

At the time of this writing, it is not known whether Theorems 6.4 and 6.5 remain true when $\mathrm{P}_{\mathrm{btt}}(A)$, $\mathrm{P}^{-1}_{\mathrm{btt}}(A)$, and $\mathcal{H}_{\mathrm{btt}}(\mathrm{E})$ are substituted for $\mathrm{P}_{\mathrm{k-tt}}(A)$, $\mathrm{P}^{-1}_{\mathrm{k-tt}}(A)$, and $\mathcal{H}_{\mathrm{k-tt}}(\mathrm{E})$, respectively. Buhrman and Mayordomo [BM95b] and, independently, Ambos-Spies, Neis, and Terwijn [ANT], have shown that the class $\mathcal{H}_{\mathrm{btt}}(\mathrm{E})$ has p_2-measure 0.

The Small $\leq^{\mathrm{P}}_{\mathrm{m}}$-Span Theorem has immediate consequences for the $\leq^{\mathrm{P}}_m$-degree structure of E and EXP.

The $\leq^{\mathrm{P}}_m$-*degree* of a language $A \subseteq \{0,1\}^*$ is the set

$$\deg^{\mathrm{P}}_m(A) = \mathrm{P}_m(A) \cap \mathrm{P}_m{}^{-1}(A).$$

Theorem 6.6 (Juedes and Lutz [JL95a]). For all $A \subseteq \{0,1\}^*$,

$$\mu(\deg^{\mathrm{P}}_m(A) \mid \mathrm{E}) = \mu(\deg^{\mathrm{P}}_m(A) \mid \mathrm{EXP}) = 0.$$

Proof. This follows immediately from Theorem 6.1. □

Theorem 6.7 (Mayordomo [May94a]). Let $\mathcal{C}_m(\mathrm{E}), \mathcal{C}_m(\mathrm{EXP})$ be the sets of languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E, EXP, respectively. Then $\mu(\mathcal{C}_m(\mathrm{E}) \mid \mathrm{E}) = \mu(\mathcal{C}_m(\mathrm{EXP}) \mid \mathrm{EXP}) = 0$.

Mayordomo's original proof of this result used Theorem 4.5 and Berman's result [Ber76] that no $\leq^{\mathrm{P}}_m$-complete language for E or EXP is P-immune. We now see that Mayordomo's result also follows from Theorem 6.3 and from Theorem 6.6.

Using Theorem 6.4 in place of Theorem 6.1 gives the following extension of Theorem 6.6.

Theorem 6.8 (Ambos-Spies, Neis, and Terwijn [ANT]). For all $A \subseteq \{0,1\}^*$ and all positive integers k,

$$\mu(deg^{\mathrm{P}}_{\mathrm{k-tt}}(A)|\mathrm{E}) = \mu(deg^{\mathrm{P}}_{\mathrm{k-tt}}(A)|\mathrm{EXP}) = 0$$

It is not currently known whether all $\leq^{\mathrm{P}}_{\mathrm{btt}}$-degrees have measure 0 in E or EXP, but this at least holds for the complete $\leq^{\mathrm{P}}_{\mathrm{btt}}$-degree.

Theorem 6.9 (Ambos-Spies, Neis, and Terwijn [ANT]). Let $\mathcal{C}_{\mathrm{btt}}(\mathrm{E}), \mathcal{C}_{\mathrm{btt}}(\mathrm{EXP})$ be the sets of languages that are $\leq^{\mathrm{P}}_{\mathrm{btt}}$-complete for E, EXP, respectively. Then $\mu(\mathcal{C}_{\mathrm{btt}}(\mathrm{E})|\mathrm{E}) = \mu(\mathcal{C}_{\mathrm{btt}}(\mathrm{EXP})|\mathrm{EXP}) = 0$.

7 Weakly hard problems

To date, our principal means of establishing the intractability of a specific computational problem has been to prove that the problem is hard for

some complexity class with respect to some class of efficient reductions. For example, a problem that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for NP, PSPACE, or some class in between is *presumably intractable* because we are inclined to believe that P $\neq$ NP. A problem that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E is *provably intractable* by the time hierarchy theorem of Hartmanis and Stearns [HS65]. In fact, problems that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E are now known to have very strong intractability properties [BS85, Huy86, KOSW94, OS86, Sch86a].

In order to extend the class of provably intractable problems, Lutz [Lut90] proposed investigation of the following measure-theoretic generalization of $\leq_{\mathrm{m}}^{\mathrm{P}}$-hardness.

Definition. A language $A \subseteq \{0,1\}^*$ is *weakly* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-hard* for E (respectively, for EXP) if $\mu(\mathrm{P}_m(A)|\mathrm{E}) \neq 0$ (respectively, $\mu(\mathrm{P}_m(A)|\mathrm{EXP}) \neq 0$).

Thus a language A is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E if a *nonnegligible subset* of the languages in E are $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to A. Clearly, every language that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E is also weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E.

Weak hardness under other classes of reductions (e.g. weak $\leq_{\mathrm{T}}^{\mathrm{P}}$-hardness) is defined analogously.

The first thing to note about weakly hard problems is that they are, indeed, intractable. Specifically, it is easy to see that $\mu(\mathrm{P}|\mathrm{E}) = \mu(\mathrm{P}|\mathrm{EXP}) = 0$ [Lut92], so we have the following.

Observation 7.1. If A is weakly $\leq_{\mathrm{T}}^{\mathrm{P}}$-hard for E, then $A \notin \mathrm{P}$.

In fact, languages that are weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E are intractable in a much stronger sense. For example, consider the following strong intractability result.

Theorem 7.2 (Orponen and Schöning [OS86]). Every language that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E has a dense P-complexity core.

The following theorem extends Theorem 7.2 (in somewhat stronger form) to all weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard languages for E.

Theorem 7.3 (Juedes and Lutz [JL95a]). Every language that is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E or EXP has a dense exponential complexity core.

Thus the weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard problems for E and EXP are, like the $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard problems, provably strongly intractable. It is then natural to ask whether there are problems that are weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard, but not $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard, for these classes. We now discuss this question and, more generally, the distribution of the weakly hard languages.

Definition. A language $A \subseteq \{0,1\}^*$ is *weakly* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-complete* for E (respectively, for EXP) if A is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E (respectively, for EXP) and $A \in \mathrm{E}$ (respectively, $A \in \mathrm{EXP}$).

As in section 6, we use the notations $\mathcal{H}_m(\mathrm{E}), \mathcal{H}_m(\mathrm{EXP}), \mathcal{C}_m(\mathrm{E})$, and $\mathcal{C}_m(\mathrm{EXP})$ to denote the classes of languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E, $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for EXP, $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E, and $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for EXP, respectively. We also use the notations $\mathcal{WH}_m(\mathrm{E}), \mathcal{WH}_m(\mathrm{EXP}), \mathcal{WC}_m(\mathrm{E})$, and $\mathcal{WC}_m(\mathrm{EXP})$ to denote the classes of languages that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E, weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for EXP, weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E, and weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for EXP, respectively.

We first discuss the known inclusions among the above-defined hardness classes. We then discuss the non-inclusions. (This was not the chronological order of discovery.) It is well known that $\mathcal{H}_m(\mathrm{E}) = \mathcal{H}_m(\mathrm{EXP})$, whence $\mathcal{C}_m(\mathrm{E}) = \mathrm{E} \cap \mathcal{C}_m(\mathrm{EXP})$. (This is clear because $\mathrm{EXP} = \mathrm{P}_m(\mathrm{E})$.) Also, Theorem 3.3 implies that $\mathcal{H}_m(\mathrm{E}) \subseteq \mathcal{WH}_m(\mathrm{E})$ and $\mathcal{H}(\mathrm{EXP}) \subseteq \mathcal{WH}_m(\mathrm{EXP})$. Using the martingale dilation technique developed by Ambos-Spies, Terwijn, and Zheng [ATZ], Juedes and Lutz proved the following.

Lemma 7.4 (Juedes and Lutz [JL95b]). Let X be a set of languages.

1. If $\mu_{\mathrm{p}_2}(\mathrm{P}_m(X)) = 0$, then $\mu_{\mathrm{p}}(X) = 0$.
2. If $\mu(\mathrm{P}_m(X)|\mathrm{EXP}) = 0$, then $\mu(X|\mathrm{E}) = 0$.

This yields the following.

Theorem 7.5 (Juedes and Lutz [JL95b]). $\mathcal{WH}_m(\mathrm{E}) \subseteq \mathcal{WH}_m(\mathrm{EXP})$.

Proof. Let $\mathrm{H} \in \mathcal{WH}_m(\mathrm{E})$. Then $\mu(\mathrm{P}_m(\mathrm{H})|\mathrm{E}) \neq 0$, so Lemma 7.4(2) with $X = \mathrm{P}_m(\mathrm{H})$ tells us that $\mu(\mathrm{P}_m(\mathrm{H})|\mathrm{EXP}) = \mu(\mathrm{P}_m(\mathrm{P}_m(\mathrm{H}))|\mathrm{EXP}) \neq 0$. Thus $\mathrm{H} \in \mathcal{WH}_m(\mathrm{EXP})$. □

The foregoing discussion, in combination with obvious facts, yields the inclusion structure depicted in Figure 3.

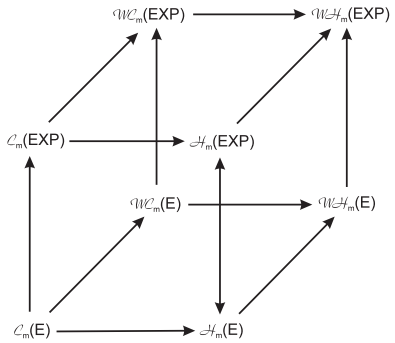

FIGURE 3. Inclusion structure of hardness classes.

We now turn to the non-inclusions. Lutz [Lut95] developed the *martingale diagonalization* technique and used it to prove the following.

Theorem 7.6 (Lutz [Lut95]). $\mathcal{C}_m(\mathrm{E}) \subsetneq \mathcal{WC}_m(\mathrm{E})$.

Corollary 7.7. $\mathcal{C}_m(\mathrm{EXP}) \subsetneq \mathcal{WC}_m(\mathrm{EXP})$.

Proof. By Theorems 7.6, 7.5, and elementary facts,

$$\mathrm{E} \cap \mathcal{C}_m(\mathrm{EXP}) = \mathcal{C}_m(\mathrm{E}) \subsetneq \mathcal{WC}_m(\mathrm{E}) \subseteq \mathrm{E} \cap \mathcal{WC}_m(\mathrm{EXP}).$$

□

Theorem 7.6 is significant because, in combination with Observation 7.1 and Theorem 7.3, it implies that the class of weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard problems for E is, indeed, a strictly larger class of provably strongly intractable problems than the class of $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard problems for E. In fact, much more is true. Juedes [Jue95] refined the martingale diagonalization of [Lut95] to prove that the class $\mathcal{WC}_m(\mathrm{E})$ does not have measure 0 in E. (By Theorem 6.7, this result implies Theorem 7.6.) More significantly, Ambos-Spies, Terwijn, and Zheng developed *martingale dilation* (a padding technique) and used it to prove the following.

Theorem 7.8 (Ambos-Spies, Terwijn, and Zheng [ATZ]).

$$\mu_{\mathrm{p}}(\mathcal{WH}_m(\mathrm{E})) = 1.$$

Corollary 7.9 (Ambos-Spies, Terwijn, and Zheng [ATZ]).

$$\mu_{\mathrm{p}_2}(\mathcal{WH}_m(\mathrm{EXP})) = 1.$$

Proof. This follows immediately from Theorems 7.8 and 7.5. □

By Theorems 7.8 and 6.7, then, almost every language in E is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, for E.

Finally, we note that the converse of Theorem 7.5 does *not* hold, even if we restrict attention to languages in E.

Theorem 7.10 (Juedes and Lutz [JL95b]). $\mathrm{E} \cap \mathcal{WC}_m(\mathrm{EXP}) \not\subseteq \mathcal{WC}_m(\mathrm{E})$.

By Theorems 7.6, 7.10, and elementary observations, Figure 3 is complete, in the sense that it depicts (either directly or via transitivity) all the inclusions that hold among these eight hardness classes.

8 Upper bounds for hard problems

We saw in Theorem 6.3 that $\leq_m^{\mathrm{P}}$-hard languages for E are very rare. As we see in this section, this is because there is a nontrivial upper bound on the sizes of complexity cores of such languages.

Recall that a language $D \subseteq \{0,1\}^*$ is *dense* if there is a real number $\varepsilon > 0$ such that $|D_{\leq n}| > 2^{n^\varepsilon}$ a.e.

The following result states that every $\leq_m^{\mathrm{P}}$-hard language for E can be decided in time 2^{4n} on a dense set of instances that can itself be decided in time 2^{4n}.

Theorem 8.1 (Juedes and Lutz [JL95a]). For every $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language H for E, there exist $B, D \in \mathrm{DTIME}(2^{4n})$ such that D is dense and $B = H \cap D$.

It is straightforward to use Theorem 8.1 to prove that $\leq_m^{\mathrm{P}}$-hard languages for E obey the following upper bound on the sizes of complexity cores.

Theorem 8.2 (Juedes and Lutz [JL95a]). Every $\mathrm{DTIME}(2^{4n})$-complexity core of every $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language for E has a dense complement.

By Corollary 5.3, almost every language in E has $\{0,1\}^*$ as a $\mathrm{DTIME}(2^{4n})$-complexity core. Thus, Theorem 8.2 says that $\leq_m^{\mathrm{P}}$-hard languages for E are *unusually simple*, in the sense that they have *unusually small* complexity cores, for languages in E. This immediately implies, and also explains, Theorems 6.3 and 6.7.

Lutz [Lut95] constructed a weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language H for E that has $\{0,1\}^*$ as a $\mathrm{DTIME}(2^{4n})$-complexity core, so Theorem 8.2 is a property of $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard languages that does *not* extend to weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard languages. In fact, by Corollary 4.3 and Theorem 7.8, almost every language in E is a weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language that does not satisfy the conclusion of Theorem 8.2.

9 Nonuniform complexity, natural proofs, and pseudorandom generators

Much remains to be discovered about the nonuniform complexities of languages in E and EXP. For example, it is a long-standing conjecture that $\mathrm{E} \not\subseteq \mathrm{P/Poly}$, i.e., that E does not have polynomial-size circuits, but it has not been proven that E does not have *linear*-size circuits, or that EXP does not have polynomial-size circuits. It is known, however, that the highest levels of circuit-size and time-bounded Kolmogorov complexity known (or provable by relativizable methods) to be exceeded infinitely often by *any* problem in EXP are in fact exceeded *almost everywhere* by *almost every*

problem in the class. Moreover, recent work of Regan, Sivakumar, and Cai [RSC95], exploiting the "natural proofs" idea of Razborov and Rudich [RR94], has shown that, if sufficiently secure pseudorandom generators exist, then these results are optimal for circuit-size complexity. We now describe these developments more fully.

Some terminology and notation will be useful. For a fixed machine M and "program" $\pi \in \{0,1\}^*$ for M, we say that "$M(\pi, n) = w$ in $\leq t$ time" if M, on input (π, n), outputs the string $w \in \{0,1\}^*$ and halts in at most t execution steps. We are especially interested in situations where the output string is of the form $w = \chi_{A_{=n}}$, i.e., the 2^n-bit characteristic string of $A_{=n}$, for some language $A \subseteq \{0,1\}^*$.

Given a machine M, a time-bound $t : \mathbf{N} \to \mathbf{N}$, a language $A \subseteq \{0,1\}^*$, and a natural number n, the *$t(n)$-time-bounded Kolmogorov complexity* of $A_{=n}$ relative to M is

$$K_M^{t(n)}(A_{=n}) = \min\left\{ |\pi| \;\middle|\; M(\pi, n) = \chi_{A_{=n}} \text{ in } \leq t(n) \text{ time} \right\}.$$

Well-known simulation techniques show that there is a machine U that is *optimal* in the sense that for each machine M there is a constant c such that, for all t, A, and n,

$$K_U^{ct(n)\log t(n)+c}(A_{=n}) \leq K_M^{t(n)}(A_{=n}) + c.$$

As is standard in this subject, we fix an optimal machine and omit it from the notation. (See [LV93] for a thorough treatment of Kolmogorov complexity.)

Theorem 9.1 (Lutz [Lut92]). If t and q are fixed polynomials, then the set of all languages A satisfying

$$K^{t(n)}(A_{=n}) > q(n) \text{ a.e.}$$

has measure 1 in EXP.

We now consider circuit-size complexity. Following standard usage (see [BDG95], for example), we define a (*Boolean*) *circuit* to be a directed acyclic graph γ with vertex set $I \cup G$, where $I = \{w_1, \ldots, w_n\}$ is the set of *inputs* ($n \geq 0$) and $G = \{g_1, \ldots, g_s\}$ is the set of *gates* ($s \geq 1$). Each input has indegree 0 and each gate has indegree 0, 1, or 2. Each gate of indegree 0 is labeled either by the constant 0 or by the constant 1. Each gate of indegree 1 is labeled either by the identity function ID: $\{0,1\} \to \{0,1\}$ or by the negation function NOT: $\{0,1\} \to \{0,1\}$. Each gate of indegree 2 is labeled either by the conjunction AND: $\{0,1\}^2 \to \{0,1\}$ or by the disjunction OR: $\{0,1\}^2 \to \{0,1\}$. The *output gate* g_s has outdegree 0. The other gates and the inputs have unrestricted outdegree. The *size* of such a circuit γ is $\text{size}(\gamma) = |G| = s$, the number of gates.

An n-input circuit γ *computes* a Boolean function $\gamma : \{0,1\}^n \to \{0,1\}$ in the usual way. For $w \in \{0,1\}^n, \gamma(w)$ is the value computed at the output gate g_s when the inputs are assigned the bits $w_1, \ldots, w_n$ of w. The *set computed by* an n-input circuit γ is then the set of all $w \in \{0,1\}^n$ such that $\gamma(w) = 1$.

The *circuit-size complexity* of a language $A \subseteq \{0,1\}^*$ is the function $\mathrm{CS}_A : \mathbf{N} \to \mathbf{N}$ defined by

$$\mathrm{CS}_A(n) = \min\{\, \mathrm{size}(\gamma) \mid \gamma \text{ computes } A_{=n} \,\}.$$

For each function $f : \mathbf{N} \to \mathbf{N}$, we define the circuit-size complexity classes

$$\begin{aligned} \mathrm{SIZE}(f) &= \{\, A \mid \mathrm{CS}_A(n) \leq f(n) \text{ a.e.} \,\}, \\ \mathrm{SIZE}^{\text{i.o.}}(f) &= \{\, A \mid \mathrm{CS}_A(n) \leq f(n) \text{ i.o.} \,\}. \end{aligned}$$

The class P/Poly is then defined by

$$\mathrm{P/Poly} = \bigcup_{k=0}^{\infty} \mathrm{SIZE}(n^k),$$

and we write

$$\mathrm{P/Poly}^{\text{i.o.}} = \bigcup_{k=0}^{\infty} \mathrm{SIZE}^{\text{i.o.}}(n^k).$$

Using a known quantitative relationship between circuit size and time-bounded Kolmogorov complexity, the following result can be derived from Theorem 9.1.

Theorem 9.2 (Lutz [Lut92]). For each fixed $k \in \mathbf{N}$, the set $\mathrm{SIZE}^{\text{i.o.}}(n^k)$ has measure 0 in EXP.

A similar argument proves the following.

Theorem 9.3 (Lutz [Lut92]). The set $\mathrm{P/Poly}^{\text{i.o.}}$ has measure 0 in the class $\mathrm{E}_3 = \mathrm{DTIME}(2^{n^{\mathrm{polylog}\, n}})$.

As noted earlier, it is a long-standing conjecture that $\mathrm{E} \not\subseteq \mathrm{P/Poly}$. Intuitively, this conjecture says that E contains problems that are *combinatorially*, as well as computationally, intractable. In light of the various strong intractability results of sections 4, 5, and 8, the stronger conjecture that P/Poly has measure 0 in E and in EXP seems to suggest itself. However, as we now explain, there is reason to be cautious about such a conjecture.

We first note that Wilson [Wil85] has exhibited oracles relative to which $\mathrm{E} \subseteq \mathrm{SIZE}(3n)$ and $\mathrm{EXP} \subseteq \mathrm{P/Poly}$, so nonrelativizable techniques will be required to prove $\mathrm{EXP} \not\subseteq \mathrm{P/Poly}$, let alone the stronger conjecture that $\mu(\mathrm{P/Poly} | \mathrm{EXP}) = 0$.

In recent years, many nonrelativizable combinatorial techniques for proving lower bounds on nonuniform complexity have been developed (see [RR94] for references to such developments), so Wilson's oracle constructions are not as daunting today as they were when he discovered them. However, all such techniques developed to date are for proving lower bounds with respect to *restricted* nonuniform models (bounded-depth circuits, monotone circuits, etc.), and do not seem to yield to lower bound techniques for general circuit-size complexity.

Razborov and Rudich [RR94] developed the notion of *natural proofs* in order to better understand these limitations on known techniques. The central idea in their work is that of a "natural combinatoral property," which we now describe, not in full generality, but in terms of the present discussion.

Definition 9.4 (Razborov and Rudich [RR94]).

1. A *combinatorial property* is a sequence $\mathcal{P} = (\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \ldots)$, where each $\mathcal{P}_n$ is a set of subsets of $\{0,1\}^n$.
2. A language $A \subseteq \{0,1\}^*$ is *drawn from* a combinatorial property $\mathcal{P}$ if, for all $n \in \mathbf{N}$, $A_{=n} \in \mathcal{P}_n$.

As part 2 of the above definition suggests, we regard each component $\mathcal{P}_n$ of a combinatorial property $\mathcal{P}$ as a "set of candidate n-slices" $A_{=n}$ for languages A that are drawn from $\mathcal{P}$. We identify each set $S \in \mathcal{P}_n$ with its 2^n-bit characteristic string χ_S, and we regard the "complexity" of $\mathcal{P}$ as the complexity of deciding membership of 2^n-bit strings in $\mathcal{P}_n$. As with martingales and measure, we will use the lower-case notations p, p_2, etc. for complexity classes of functions whose inputs are characteristic sequences. At present, we are interested in nonuniform p_2-complexity, where the nonuniformity is provided by an advice function.

Definition. A *nonuniform* p_2*-advice function* is a function $h : \mathbf{N} \to \{0,1\}^*$ for which there is a constant $k \in \mathbf{N}$ such that, for all $n > 0, |h(n)| \leq k + 2^{(\log n)^k}$. (Note that h need not be computable; this is the nonuniformity.)

Definition. A combinatorial property $\mathcal{P}$ is *nonuniformly* p_2*-decidable* if there exist a nonuniform p_2-advice function h and a function $f \in \mathrm{p}_2$ such that, for all $n \in \mathbf{N}$ and $S \subseteq \{0,1\}^n$,

$$f(\chi_S, h(2^n)) = [\![\chi_S \in \mathcal{P}_n]\!].$$

In a lower bound argument, the typical role of a combinatorial property is to reliably diagonalize against some complexity class.

Definition 9.5 (Razborov and Rudich [RR94]). Let $\mathcal{P}$ be acombinatorial property, and let $\mathcal{C}$ be a class of languages.

1. $\mathcal{P}$ is *useful infinitely often (useful i.o.) against* $\mathcal{C}$ if, for every $A \in \mathcal{C}$, there exist infinitely many $n \in \mathbf{N}$ such that $A_{=n} \notin \mathcal{P}_n$.
2. $\mathcal{P}$ is *useful almost everywhere (useful a.e.) against* $\mathcal{C}$ if, for every $A \in \mathcal{C}$, for all sufficiently large $n \in \mathbf{N}$, $A_{=n} \notin \mathcal{P}_n$.

The crucial thing that Razborov and Rudich observed is that the combinatorial properties used in lower bound proofs are typically large, in the following sense.

Definition 9.6 (Razborov and Rudich [RR94]). A combinatorial property $\mathcal{P}$ is *large* if there is a constant $k \in \mathbf{N}$ such that, for all sufficiently large $n \in \mathbf{N}$,

$$| \mathcal{P}_n | \geq 2^{2^n - kn}.$$

To rephrase the definition probabilistically, let $\Pr(\mathcal{P}_n)$ denote the probability that $S \in \mathcal{P}_n$ when $S \subseteq \{0,1\}^n$ is chosen according to a random experiment in which all subsets of $\{0,1\}^n$ are equally probable. Then $\mathcal{P}$ is large if there exists k such that, for all sufficiently large n, $\Pr(\mathcal{P}_n) \geq 2^{-kn}$.

We now have all the elements of the notion of a "natural combinatorial property."

Definition 9.7 (Razborov and Rudich [RR94]). A combinatorial property $\mathcal{P}$ is *nonuniformly* p_2*-natural i.o. against* a class $\mathcal{C}$ of languages if $\mathcal{P}$ is nonuniformly p_2-decidable, $\mathcal{P}$ is useful i.o. against $\mathcal{C}$, and $\mathcal{P}$ is large.

Here we are specifically interested in the EXP versus P/Poly question, so we have specialized the above definition to nonuniform p_2-decidability and i.o. diagonalization. The interested reader is referred to [RR94, Raz] for more general aspects of Razborov and Rudich's work.

Regan, Sivakumar, and Cai's work on natural combinatorial properties involves the existence of a certain kind of secure pseudorandom generator. We now develop the required definitions.

Definition. Let p be a polynomial such that $p(n) \geq n+1$. A $p(n)$*-generator* is a function $g \in \mathrm{PF}$ such that, for all $x \in \{0,1\}^*$, $| g(x) | = p(|x|)$.

Intuitively a generator g, given a short, random *seed* x, outputs a long, hopefully pseudorandom, string $g(x)$. The desired notion of pseudorandomness, also called "security," is given by the following definition, due to Yao [Yao82].

Definition. Let $s = \mathbf{N} \to \mathbf{N}$. A $p(n)$-generator g is *nonuniformly* $s(n)$*-secure* if, for every sufficiently large $n \in \mathbf{N}$, for every $p(n)$-input, 1-output circuit γ with $size(\gamma) \leq s(n)$,

$$| \Pr[\gamma(g(x)) = 1] - \Pr[\gamma(y) = 1] | < \frac{1}{s(n)},$$

where the probabilities are computed according to the uniform distributions on $x \in \{0,1\}^n$ and $y \in \{0,1\}^{p(n)}$, respectively.

Intuitively, a generator g is $s(n)$-secure if no $s(n)$-gate circuit can statistically distinguish the uniform distribution on $\{0,1\}^{p(n)}$ from the distribution induced on $\{0,1\}^{p(n)}$ by the generator g with the uniform distribution on the seed space $\{0,1\}^n$.

Definition.

1. A $p(n)$-generator g is *nonuniformly polynomially secure* if g is $s(n)$-secure for every polynomial s.
2. A $p(n)$-generator g is *nonuniformly exponentially secure* if there is a real constant $\delta > 0$ such that g is 2^{n^δ}-secure.

It is easy to show that, if there exists a nonuniformly polynomially secure $p(n)$-generator g, then NP $\not\subseteq$ P/Poly (whence P $\neq$ NP). In fact, such generators are widely conjectured to exist. The existence of $p(n)$-generators that are nonuniformly exponentially secure is an even stronger conjecture, but not entirely implausible. For example, Regan, Sivakumar, and Cai [RSC95] have pointed out that the smallest circuits known to break pseudorandom generators that are based on the discrete logarithm problem have nearly $2^{\sqrt{n}}$ gates.

In any case, the following result shows that the existence of nonuniformly exponentially secure generators is not consistent with the existence of nonuniformly p_2-natural properties against P/Poly.

Theorem 9.8 (Razborov [Raz]; see also [RSC95]). If there is a nonuniformly exponentially secure $2n$-generator, then there is no combinatorial property that is nonuniformly p_2-natural i.o. against P/Poly.

The following result relates these issues to the measure of P/Poly in EXP.

Theorem 9.9 (Regan, Sivakumar, and Cai [RSC95]). If $\mu(\mathrm{P/Poly}|\mathrm{EXP}) = 0$, then there is a combinatorial property that is nonuniformly p_2-natural i.o. against P/Poly.

By Theorems 9.4 and 9.5, we have the following.

Theorem 9.10 (Regan, Sivakumar, and Cai [RSC95]). If there is a nonuniformly exponentially secure $2n$-generator, then $\mu(\mathrm{P/Poly}|\mathrm{EXP}) \neq 0$.

By Lemma 7.4, $\mu(\mathrm{P/Poly}|\mathrm{EXP}) = 0$ implies that $\mu(\mathrm{P/Poly}|\mathrm{E}) = 0$. At the time of this writing, the converse is not known to hold, nor is an analogue of Theorem 9.6 known to hold for E. It is thus conceivable that P/Poly has measure 0 in E and (by Theorem 9.3) in E_3, but not in $\mathrm{E}_2 = \mathrm{EXP}$.

10 Weak stochasticity

It is now known that almost every language in E, and almost every language in E_2, is statistically unpredictable by feasible deterministic algorithms, even with some nonuniform advice. This result, which appears to be very useful, is explained in this section.

Properties defined in terms of limiting frequencies of failure of prediction schemes are called *stochasticity* properties in the terminology of Kolmogorov [KU87, USS90]. (Such properties were originally proposed by von Mises [vM39] and Church [Chu40] in their efforts to define randomness.) Because the prediction schemes allowed in this section are of a restricted sort, the property discussed here is a *weak stochasticity* property.

We now make our terminology precise. Our notion of advice classes is standard [KL80]. An *advice function* is a function $h : \mathbf{N} \to \{0,1\}^*$. Given a function $q : \mathbf{N} \to \mathbf{N}$, we write $\mathrm{ADV}(q)$ for the set of all advice functions h such that $|h(n)| \leq q(n)$ for all $n \in \mathbf{N}$. Given a language $A \subseteq \{0,1\}^*$ and an advice function h, we define the language A/h ("A with advice h") by

$$A/h = \{x \in \{0,1\}^* \mid \langle x, h(|x|)\rangle \in A\}.$$

Given functions $t, q : \mathbf{N} \to \mathbf{N}$, we define the *advice class*

$$\mathrm{DTIME}(t)/\mathrm{ADV}(q) = \{A/h \mid A \in \mathrm{DTIME}(t), h \in \mathrm{ADV}(q)\}.$$

Definition. Let $t, q, \nu : \mathbf{N} \to \mathbf{N}$ and let $A \subseteq \{0,1\}^*$. Then A is *weakly (t,q,ν)-stochastic* if, for all $B, C \in \mathrm{DTIME}(t)/\mathrm{ADV}(q)$ such that $|C_{=n}| \geq \nu(n)$ for all sufficiently large n,

$$\lim_{n\to\infty} \frac{|(A \triangle B) \cap C_{=n}|}{|C_{=n}|} = \frac{1}{2}.$$

Intuitively, B and C together form a "prediction scheme" in which B tries to guess the behavior of A on the set C. A is weakly (t,q,ν)-stochastic if no such scheme is better in the limit than guessing by random tosses of a fair coin. (This definition is slightly stronger than the weak stochasticity defined in [LM94], in that the language C is allowed advice here.)

Theorem 10.1 (Weak Stochasticity Theorem—Lutz and Mayordomo [LM94]). For every fixed $k \in \mathbf{N}$ and every fixed real number $\nu > 0$,

$$\mu(\mathrm{WS}(2^{kn}, kn, 2^{\nu n})|\mathrm{E}) \quad = \quad \mu_{\mathrm{p}}(WS(2^{kn}, kn, 2^{\nu n})) = 1$$

and

$$\mu_{\mathrm{p}_2}(WS(2^{n^k}, n^k, 2^{n^\nu})) \quad = \quad \mu(\mathrm{WS}(2^{n^k}, n^k, 2^{n^\nu})|\mathrm{EXP}) = 1.$$

That is, almost every language in E, and almost every language in EXP, is weakly stochastic with the indicated parameters.

Regan and Sivakumar [RS95] have recently given a more precise analysis of the Weak Stochasticity Theorem, especially with respect to the rate of convergence.

11 Density of hard languages

As noted in section 9 above, it is a long-standing open conjecture that $\mathrm{E} \not\subseteq \mathrm{P/Poly}$, i.e., that not every language in E has polynomial circuit-size complexity. Many ongoing efforts to prove this conjecture follow a program that began with the following results of Meyer.

Recall that a language $A \subseteq \{0,1\}^*$ is *sparse* if there is a polynomial q such that $|A_{\leq n}| \leq q(n)$ a.e., and *dense* if there is a real number $\varepsilon > 0$ such that $|A_{\leq n}| > 2^{n^\varepsilon}$ a.e. We write SPARSE for the set of all sparse languages and DENSE for the set of all dense languages. Note that $\mathrm{SPARSE} \subsetneq \mathrm{DENSE}^c$, where DENSE^c is the complement of DENSE. For each reducibility $\leq_r^{\mathrm{P}}$, each language A, and each set $\mathcal{S}$ of languages, we write

$$\mathrm{P}_r(A) = \{\, B \mid B \leq_r^{\mathrm{P}} A \,\}$$

and

$$\mathrm{P}_r(\mathcal{S}) = \bigcup_{A \in \mathcal{S}} \mathrm{P}_r(\mathcal{S}).$$

Theorem 11.1 (Meyer [Mey77]). $\mathrm{P/Poly} = \mathrm{P}_{\mathrm{T}}(\mathrm{SPARSE})$.

Theorem 11.2 (Meyer [Mey77]). Every $\leq_m^{\mathrm{P}}$-hard language for E (or any larger class) is dense. That is, $\mathrm{E} \not\subseteq \mathrm{P}_m(\mathrm{DENSE}^c)$.

Corollary 11.3 (Meyer [Mey77]). $\mathrm{E} \not\subseteq \mathrm{P}_m(\mathrm{SPARSE})$.

Meyer's results suggest proving theorems of the form

$$\mathrm{E} \not\subseteq \mathrm{P}_r(\mathrm{SPARSE})$$

for successively larger classes $\mathrm{P}_r(\mathrm{SPARSE})$ in the range

$$\mathrm{P}_m(\mathrm{SPARSE}) \subseteq \mathrm{P}_r(\mathrm{SPARSE}) \subseteq \mathrm{P}_{\mathrm{T}}(\mathrm{SPARSE}).$$

Along the way, we should try to make our results as strong as possible. (For example, results of Nisan and Wigderson [NW88, Nis92] indicate that sufficiently strong lower bounds on the nonuniform complexity of E could lead to the construction of useful pseudorandom generators.)

The next big step in this program was taken by Watanabe, who proved the following result concerning $\leq_{q(n)-tt}^{\mathrm{P}}$-reducibility (polynomial-time truth-table reducibility with $q(n)$ queries on inputs of length n).

Theorem 11.4 (Watanabe [Wat87b]). Every $\leq^{\mathrm{P}}_{O(\log n)-tt}$-hard language for E is dense. That is, $\mathrm{E} \not\subseteq \mathrm{P}_{O(\log n)\text{-}tt}(\mathrm{DENSE}^c)$.

Recently, a measure-theoretic attack on this problem has led to the following strengthening of Theorem 11.4.

Theorem 11.5 (Lutz and Mayordomo [LM94]). For every real number $\alpha < 1$ (e.g., $\alpha = 0.99$), $\mu(\mathrm{P}_{n^\alpha-tt}(\mathrm{DENSE}^c) \mid \mathrm{E}) = \mu(\mathrm{P}_{n^\alpha-tt}(\mathrm{DENSE}^c) \mid \mathrm{EXP}) = 0$.

Corollary 11.6 (Lutz and Mayordomo [LM94]). For every real number $\alpha < 1$ (e.g., $\alpha = 0.99$), $\mathrm{E} \not\subseteq \mathrm{P}_{n^\alpha-tt}(\mathrm{DENSE}^c)$, i.e., every $\leq^{\mathrm{P}}_{n^\alpha-tt}$-hard language for E is dense.

The proof of Theorem 11.5 uses a simple combinatorial technique—the *sequentially most frequent query selection*—to show that every language in $\mathrm{P}_{n^\alpha-tt}(\mathrm{DENSE}^c)$ is predictable, i.e., fails to be weakly stochastic with suitable parameters. The result then follows immediately from Theorem 10.1, the Weak Stochasticity Theorem.

Given the Weak Stochasticity Theorem, which is a very general principle, this proof of Corollary 11.6 (via Theorem 11.5) is much simpler than the stage construction originally used to prove Theorem 11.4. This is not surprising, once it is noted that our proof of Corollary 11.6 is an application of (a resource-bounded generalization of) the probabilistic method [Erd47, Sha48, Sha49, ES74, Spe87, AS92], which exploits the fact that it is often easier to establish the *abundance* of objects of a given type than to construct a *specific* object of that type.

It should be emphasized here that Theorem 11.5 is more than a means of proving Corollary 11.6. (By analogy, the value of classical Lebesgue measure and probability far surpasses their role as tools for existence proofs.) The quantitative content of Theorem 11.5—that the set $\mathrm{P}_{n^\alpha-tt}(\mathrm{DENSE}^c) \cap \mathrm{E}$ is a *negligibly small* subset of E—is much stronger than the qualitative separation of Corollary 11.6.

Recently, Fu has independently proven the following, related result.

Theorem 11.7 (Fu [Fu95]).

1. For every real $\alpha < \frac{1}{4}$, $\mathrm{E} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE}^c)$.

2. For every real $\alpha < 1$, $\mathrm{EXP} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE}^c)$.

Note that the reducibilities here are Turing, i.e., adaptive, as opposed to the nonadaptive truth-table reducibilities of Corollary 11.6.

$$\begin{array}{ccc}
\mu(\mathrm{NP} \mid \mathrm{EXP}) \neq 0 & \Longleftarrow & \mu(\mathrm{NP} \mid \mathrm{E}) \neq 0 \\
\Updownarrow & & \Downarrow \\
\mu_{\mathrm{p}_2}(\mathrm{NP}) \neq 0 & \Longrightarrow & \mu_{\mathrm{p}}(\mathrm{NP}) \neq 0 \\
\Downarrow & & \Downarrow \\
(\forall k)\, \mathrm{NP} \not\subseteq \mathrm{DTIME}(2^{n^k}) & \Longrightarrow & (\forall c)\, \mathrm{NP} \not\subseteq \mathrm{DTIME}(2^{cn}) \\
 & & \Downarrow \\
 & & \mathrm{P} \neq \mathrm{NP}
\end{array}$$

FIGURE 4. Non-smallness conditions for NP.

12 Strong hypotheses

At our present state of knowledge (i.e., lack thereof), many results in complexity theory contain strong, unproven hypotheses. Here are just three examples.

Theorem 12.1 (Karp and Lipton [KL80]). If $\Sigma_2^{\mathrm{P}} \neq \Pi_2^{\mathrm{P}}$, then $\mathrm{NP} \not\subseteq \mathrm{P}_{\mathrm{T}}(\mathrm{SPARSE})$.

Theorem 12.2 (Mahaney [Mah82]). If $\mathrm{P} \neq \mathrm{NP}$, then $\mathrm{NP} \not\subseteq \mathrm{P}_m(\mathrm{SPARSE})$.

Theorem 12.3 (Ogiwara and Watanabe [OW91]). If $\mathrm{P} \neq \mathrm{NP}$, then $\mathrm{NP} \not\subseteq \mathrm{P}_{btt}(\mathrm{SPARSE})$.

(This last result refers to polynomial-time truth-table reducibility with an arbitrary but fixed number of queries.)

The proofs of the above three theorems have given complexity theory some its most beautiful and useful techniques. However, the conclusions of these theorems are far weaker than the observation that *all known* $\leq_{\mathrm{T}}^{\mathrm{P}}$*-hard languages for* NP *are dense*. In this sense, relative to our current knowledge, the hypotheses $\mathrm{P} \neq \mathrm{NP}$ and $\Sigma^{\mathrm{P}} \neq \Pi_2^{\mathrm{P}}$ lack explanatory power.

In order to make progress on matters of this type, we have proposed investigation of various strong measure-theoretic hypotheses. For example, Figure 4 gives the implications among various conditions asserting the non-smallness of NP. In this section we briefly discuss the reasonableness and known consequences of the weakest measure-theoretic hypothesis in Figure 4, namely, the hypothesis that NP does not have p-measure 0.

This hypothesis is best understood by considering the meaning of its negation, that NP has p-measure 0. This latter condition occurs if and only if there is a p-martingale that succeeds (bets successfully) on every language $A \in \mathrm{NP}$. The fact that the strategy d is p-computable means that, when betting on the condition "$x \in A$", d requires only $2^{c|x|}$ time for some fixed constant c. (This is because the running time of d for this bet is

polynomial in the number of predecessors of x in the standard ordering of $\{0,1\}^*$). On the other hand, for all $k \in \mathbf{N}$, there exist languages $A \in \mathrm{NP}$ with the property that the apparent search space (space of witnesses) for each input x has $2^{|x|^k}$ elements. Since c is fixed, we have $x^{cn} \ll x^{n^k}$ for large values of k. Such a martingale d would thus be a very remarkable algorithm! It would bet successfully on *all* NP languages, using far less than enough time to examine the search spaces of most such languages. It is reasonable to conjecture that no such martingale exists, i.e., that NP does not have p-measure 0.

Kautz and Miltersen [KM94] have shown that, if A is an algorithmically random oracle, then $\mu_{\mathrm{p}^A}(\mathrm{NP}^A) \neq 0$. This proof, though interesting for its analysis of independence and randomness, gives no evidence for the truth of the unrelativized $\mu_p(\mathrm{NP}) \neq 0$ conjecture.

Since $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ implies $\mathrm{P} \neq \mathrm{NP}$, and $\mu_{\mathrm{p}}(\mathrm{NP}) = 0$ implies $\mathrm{NP} \neq \mathrm{EXP}$, we are unable to prove or disprove the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ conjecture at this time. Until such a mathematical resolution is available, the condition $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is best investigated as a *scientific hypothesis*, to be evaluated in terms of the extent and credibility of its consequences.

We now survey known consequences of the hypothesis that NP does not have p-measure 0. The first follows immediately from Theorem 4.5.

Theorem 12.4 (Mayordomo [May94a]). If NP does not have measure 0, then NP contains a P-bi-immune language.

Using standard techniques, the following result has been derived from Theorem 12.4.

Theorem 12.5 (Lutz and Mayordomo [LM]). If NP does not have p-measure 0, then $\mathrm{E} \neq \mathrm{NE}$ and $\mathrm{EE} \neq \mathrm{NEE}$.

Corollary 12.6 (Lutz and Mayordomo [LM]). If NP does not have p-measure 0, then there is an NP search problem that does not reduce to the corresponding decision problem.

Proof. Bellare and Goldwasser [BG94] have shown that, if $\mathrm{EE} \neq \mathrm{NEE}$, then there is an NP search problem that does not reduce to the corresponding decision problem. The present corollary follows immediately from this and Theorem 12.5. □

We now consider complexity cores of languages that are $\leq^{\mathrm{P}}_m$-hard for NP. The following result is well-known.

Theorem 12.7 (Orponen and Schöning [OS86]). If $\mathrm{P} \neq \mathrm{NP}$, then every language that is $\leq^{\mathrm{P}}_m$-hard for NP has a nonsparse P-complexity core.

Strengthening the hypothesis of Theorem 12.7 gives a stronger conclusion. (This essentially follows from Theorem 7.3.)

Theorem 12.8 (Juedes and Lutz [JL95a]). If NP does not have p-measure 0, then every language that is $\leq^{\mathrm{P}}_m$-hard for NP has a dense exponential complexity core.

Concerning the density of hard languages for NP, Theorem 11.5 gives us the following result. Note that the hypothesis and conclusion are both stronger than in Theorem 12.6.

Theorem 12.9 (Lutz and Mayordomo [LM94]). If NP does not have p-measure 0, then for every real number $\alpha < 1$, NP $\not\subseteq \mathrm{P}_{n^\alpha - tt}(\mathrm{DENSE}^c)$, i.e., every $\leq^{\mathrm{P}}_{n^\alpha - tt}$-hard language for NP is dense.

The next result concerns NP-completeness. The NP-completeness of decision problems has two principal, well-known formulations. These are the $\leq^{\mathrm{P}}_{\mathrm{T}}$-completeness introduced by Cook [Coo71] and the $\leq^{\mathrm{P}}_m$-completeness introduced by Karp [Kar72] and Levin [Lev73]. It is widely conjectured ([LLS75, You83, LY90, Hom90]) that these two notions are distinct:

CvKL Conjecture. ("Cook versus Karp-Levin"). There exists a language that is $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, but not $\leq^{\mathrm{P}}_m$-complete, for NP.

The CvKL Conjecture is very ambitious, since it implies that P $\neq$ NP. The question has thus been raised [LLS75, Sel79, Hom90, BHT91] whether the CvKL Conjecture can be derived from some reasonable complexity-theoretic hypothesis, such as P $\neq$ NP or the separation of the polynomial-time hierarchy into infinitely many levels. To date, despite extensive work [Sel79, KM75, Wat87a, Wat87b, WT92, Wat87b, BHT91, LY90, LLS75, Sel79, Hom90, BHT91] , even this more modest objective has not been achieved.

The following result shows that the CvKL Conjecture holds under our strong measure-theoretic hypothesis.

Theorem 12.10 (Lutz and Mayordomo [LM]). If NP does not have p-measure 0, then there is a language C that is $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, but not $\leq^{\mathrm{P}}_m$-complete for NP.

Of the measure-theoretic results mentioned thus far in this section, Theorems 12.4, 12.8, and 12.9 hold with NP replaced by any class whatsoever. Theorem 12.5, Corollary 12.6, and Theorem 12.10 are more specific to NP.

The hypothesis $\mu_p(\mathrm{NP}) \neq 0$ also has consequences involving the complexity classes BPP and $\mathrm{BPP}(\Sigma^{\mathrm{P}}_k)$ for $k \geq 1$. In fact, these consequences all follow from the hypothesis that the class Δ^{P}_2 does not have p-measure

0. Since NP $\subseteq \Delta_2^{\mathrm{P}}$, the hypothesis $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$ follows from, and is thus at least as plausible as, the hypothesis $\mu_p(\mathrm{NP}) \neq 0$.

The first consequence of $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$ is a tightening of the result, due to Lautemann [Lau83] and Sipser and Gács [Sip83], that BPP $\subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$.

Theorem 12.11 (Allender and Strauss [AS94]). If $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$, then BPP $\subseteq \Delta_2^{\mathrm{P}}$.

A slight strengthening of the proof of Theorem 12.11 yields the following.

Theorem 12.12 (Lutz [Luta]). If $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$, then for all $k \geq 1$, $\mathrm{BPP}(\Sigma_k^{\mathrm{P}}) = \Delta_{k+1}^{\mathrm{P}}$.

Theorem 12.12 has consequences for lowness and polynomial advice. If $\mathcal{C}$ and $\mathcal{L}$ are classes of languages, then $\mathcal{L}$ is *low* for $\mathcal{C}$ if $\mathcal{C}(\mathcal{L}) \subseteq \mathcal{C}$. The following corollary follows easily from Theorem 12.12 and the fact, due to Köbler, Schöning, and Torán [KST93], that AM $\cap$ co-AM is low for AM. (See [KST93] for the definition and basic properties of the "Arthur-Merlin" class AM.)

Corollary 12.13 (Lutz [Luta]). If $\mu_($ $\Delta_2^{\mathrm{P}}) \neq 0$, then AM $\cap$ co-AM is low for Δ_2^{P}.

Corollary 12.14 (Lutz [Luta]). If $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$, then BPP is low for Δ_2^{P}.

Corollary 12.15 (Lutz [Luta]). Assume that $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$. Then the graph isomorphism problem is low for Δ_2^{P}. Thus, if $\Delta_2^{\mathrm{P}} \neq$ PH, then the graph isomorphism problem is not $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, or even $\leq_{\mathrm{T}}^{\mathrm{SNP}}$-complete for NP.

(The strong nondeterministic polynomial-time reducibility $\leq_{\mathrm{T}}^{\mathrm{SNP}}$ is defined by $A \leq_{\mathrm{T}}^{\mathrm{SNP}} B$ if and only if $A \in \mathrm{NP}(B) \cap \text{co-NP}(B)$.)

By Theorem 11.1, Theorem 12.1 says that, if $\Sigma_2^{\mathrm{P}} \neq$ PH, then NP $\not\subseteq$ P/Poly. A recent, significant improvement of this result is the following.

Theorem 12.16.[BCKT94, KW95] If ZPP(NP) $\neq$ PH then NP $\not\subseteq$ P/Poly.

(See [BDG95] for the definition and basic properties of the zero-error probabilistic polynomial-time complexity class ZPP. It is well-known that $\Delta_2^{\mathrm{P}} \subseteq \mathrm{ZPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$.)

The following result, which follows immediately from Theorems 12.12 and 12.16, derives the same conclusion as Theorems 12.1 and 12.16 from a somewhat different hypothesis.

Corollary 12.17 (Lutz [Luta]). If $\mu_p(\Delta_2^{\mathrm{P}}) \neq 0$ and $\Delta_2^{\mathrm{P}} \neq$ PH, then NP $\not\subseteq$ P/Poly.

13 Conclusion

Resource-bounded measure has been shown to interact in informative, quantitative ways with polynomial-time reductions, bi-immunity, complexity cores, completeness, circuit complexity, Kolmogorov complexity, the density of hard languages, randomized complexity, lowness, and other much-studied structural aspects of the exponential time complexity classes E and EXP. This work has expanded the class of provably intractable problems (section 7), and there are indications throughout that it may have profound implications for the structure of NP and other classes that characterize important computational problems.

Ultimately, the objective of this work is a detailed account of the quantitative structure of E and EXP, with sufficient resolution to yield useful bounds on the complexities of natural computational problems. The results achieved to date are only a very small beginning. Here we mention just a few directions for further work.

1. One of the most significant challenges is to find *natural* examples of languages that are weakly $\leq_m^P$-complete, but not $\leq_m^P$-complete, for EXP. Theorem 7.8 suggests the existence of such natural examples, and Theorem 7.3 underscores the importance of finding them.

2. Most of the results mentioned in sections 4-8 concern the structure of E and EXP under $\leq_m^P$-reducibility. It will be worthwhile to investigate how far in the direction of $\leq_T^P$-reducibility these results can be extended. For example, a Small Span Theorem for $\leq_T^P$-reductions (or even for $\leq_{tt}^P$-reductions) in EXP would imply that EXP $\not\subseteq$ BPP [JL95a, ANT].

3. In light of Theorem 11.4 and Corollary 11.6, it may well be that measure arguments can be used to simplify or replace other known stage constructions. Such simplification might clarify issues, leading to further progress.

4. *Many* other structural aspects of E and EXP remain to be investigated from the standpoint of resource-bounded measure. For example, it seems likely that resource-bounded measure will shed light on the theory of average-case complexity. Cai and Selman [CS96] have made one observation in this regard, but we hope that this is only a beginning.

5. Work to date has focused on the measure-theoretic structure of classes of languages, i.e., decision problems. Classes of functions, search problems, optimization problems, approximation problems, etc., should also be investigated in this light.

6. The reasonableness and consequences of strong hypotheses such as those mentioned in section 12 require further investigation. Are the

hypotheses $\mu_{\rm p}({\rm NP}) \neq 0$ and $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$ equivalent, or is the latter in some sense weaker? Does $\mu_{\rm p}({\rm NP}) \neq 0$ imply that there is a language that is $\leq_{\rm T}^{\rm P}$-complete, but not $\leq_{\rm tt}^{\rm P}$-complete, for NP? Do these hypotheses have unreasonable consequences? Many significant questions remain.

7. Ambos-Spies, Neis, and Terwijn [ANT] have recently shown that the notion of resource-bounded genericity introduced by Ambos-Spies, Fleischhack, and Huwig [AFH87, AFH88] interacts very usefully with resource-bounded measure. (See [Amb95] for a survey of this and other types of resource-bounded genericity.) Balcázar and Mayordomo [BM95a] have characterized this genericity as a strong kind of bi-immunity, and Ambos-Spies, Mayordomo, Wang, and Zheng [AMWZ96] have further investigated the relationships between genericity and measure, but more investigation is needed to fully understand the relative power of these two methods.

8. One of the most challenging tasks remaining is the development of measure in subexponential complexity classes. Mayordomo [May94c, May94b] and Allender and Strauss [AS94] have proposed (inequivalent) definitions of measure in PSPACE, and Allender and Strauss [AS94, AS95] have investigated various formulations of measure in P and other subexponential classes, but at the time of this writing, many issues are unresolved.

Resource-bounded measure is a powerful generalization of Lebesgue measure. There is reason to hope that it will be as fruitful in complexity theory as Lebesgue measure has been in analysis and mathematical physics. Many investigators will have to ask and answer many questions in order for resource-bounded measure to achieve its full potential.

Acknowledgments

I thank many colleagues and students for fun and helpful discussions over the past few years. I especially thank my colleagues David Juedes and Elvira Mayordomo for working with me in this area, and for allowing me to include so much of our work in this survey. I also thank a referee for numerous valuable improvments in the exposition.

14 References

[AFH87] K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizing over polynomial time computable sets. *Theoretical Computer Science*, 51:177–204, 1987.

[AFH88] K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizing over deterministic polynomial time. In *Proceedings of Computer Science Logic '87*, pages 1–16. Springer-Verlag, 1988.

[Amb86] K. Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. In *Proceedings of the First Structure in Complexity Theory Conference*, pages 23–34. Springer-Verlag, 1986.

[Amb95] K. Ambos-Spies. Resource-bounded genericity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference*, pages 162–181. IEEE Computer Society Press, 1995.

[AMWZ96] K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. In *Proceedings of the Thirteenth Symposium on Theoretical Aspects of Computer Science*, pages 63–74. Springer-Verlag, 1996.

[ANT] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*. To appear.

[AS92] N. Alon and J. H. Spencer. *The Probabilistic Method*. Wiley, 1992.

[AS94] E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, pages 807–818. IEEE Computer Society Press, 1994.

[AS95] E. Allender and M. Strauss. Measure on P : Robustness of the notion. In *Proceedings of the 20th International Symposium on Mathematical Foundations of Computer Science*, pages 129–138. Springer-Verlag, 1995.

[ATZ] K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource-bounded randomness and weakly complete problems. *Theoretical Computer Science*. To appear.

[BCKT94] N. H. Bshouty, R. Cleve, S. Kannan, and C. Tamon. Oracles and queries that are sufficient for exact learning. In *Proceedings of the Seventh ACM Conference on Computational Learning Theory*, pages 130–139. ACM Press, 1994.

[BDG90] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II*. Springer-Verlag, 1990.

[BDG95] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*. Springer-Verlag, Berlin, 1995. Second edition.

[Ber76] L. Berman. On the structure of complete sets: Almost everywhere complexity and infinitely often speedup. In *Proceedings of the Seventeenth Annual Conference on Foundations of Computer Science*, pages 76–80, 1976.

[BG94] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM Journal on Computing*, 23:97–119, 1994.

[BH77] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 6:305–322, 1977.

[BHT91] H. Buhrman, S. Homer, and L. Torenvliet. Completeness for nondeterministic complexity classes. *Mathematical Systems Theory*, 24:179–200, 1991.

[BL96] H. Burman and L. Longpré. Compressibility and resource bounded measure. In *Proceedings of the Thirteenth Symposium on Theoretical Aspects of Computer Science*, pages 13–24. Springer-Verlag, 1996.

[BM95a] J. L. Balcázar and E. Mayordomo. A note on genericity and bi-immunity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference*, pages 193–196. IEEE Computer Society Press, 1995.

[BM95b] H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference*, pages 197–203. IEEE Computer Society Press, 1995.

[BS85] J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Mathematical Systems Theory*, 18:1–10, 1985.

[Chu40] A. Church. On the concept of a random sequence. *Bulletin of the American Mathematical Society*, 46:130–135, 1940.

[Coo71] S. A. Cook. The complexity of theorem proving procedures. In *Proceedings of the Third ACM Symposium on Theory of Computing*, pages 151–158, 1971.

[CS96] J. Cai and A. L. Selman. Fine separation of average time complexity classes. In *Proceedings of the Thirteenth Symposium on Theoretical Aspects of Computer Science*, pages 331–343. Springer-Verlag, 1996.

[Erd47] P. Erdös. Some remarks on the theory of graphs. *Bulletin of the American Mathematical Society*, 53:292–294, 1947.

[ES74] P. Erdös and J. Spencer. *Probabilistic Methods in Combinatorics*. Academic Press, New York, 1974.

[Fen91] S. A. Fenner. Notions of resource-bounded category and genericity. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference*, pages 196–212. IEEE Press, 1991.

[Fen95] S. A. Fenner. Resource-bounded category: a stronger approach. In *Proceedings of the Tenth Structure in Complexity Theory Conference*, pages 182–192. IEEE Computer Society Press, 1995.

[Fre72] R. I. Freidzon. Families of recursive predicates of measure zero. Translated in *Journal of Soviet Mathematics*, 6(1976):449–455, 1972.

[Fu95] B. Fu. With quasi-linear queries, EXP is not polynomial time Turing reducible to sparse sets. *SIAM Journal on Computing*, 24:1082–1090, 1995.

[Hal50] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1950.

[Hom90] S. Homer. Structural properties of nondeterministic complete sets. In *Proceedings of the Fifth Annual Structure in Complexity Theory Conference*, pages 3–10, 1990.

[HS65] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Transactions of the American Mathematical Society*, 117:285–306, 1965.

[Huy86] D. T. Huynh. Some observations about the randomness of hard problems. *SIAM Journal on Computing*, 15:1101–1105, 1986.

[JL95a] D. W. Juedes and J. H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24(2):279–295, 1995.

[JL95b] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science*, 143:149–158, 1995.

[Jue94] D. W. Juedes. *The Complexity and Distribution of Computationally Useful Problems*. PhD thesis, Iowa State University, 1994.

[Jue95] D. W. Juedes. Weakly complete problems are not rare. *Computational Complexity*, 5:267–283, 1995.

[Kar72] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–104. Plenum Press, 1972.

[KL80] R. M. Karp and R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th ACM Symposium on Theory of Computing*, pages 302–309, 1980. Also published as Turing machines that take advice, *L'Enseignement Mathematique* **28** (1982), pp. 191–209.

[KM75] K. Ko and D. Moore. Completeness, approximation and density. *Journal of the ACM*, 22:787–796, 1975.

[KM94] S. M. Kautz and P. B. Miltersen. Relative to a random oracle, NP is not small. In *Proceedings of the Ninth Annual Structure in Complexity Theory Conference*, pages 162–174. IEEE Computer Society Press, 1994.

[KOSW94] K. Ko, P. Orponen, U. Schöning, and O. Watanabe. Instance complexity. *Journal of the Association of Computing Machinery*, 41:96–121, 1994.

[KST93] J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism Problem.* Birkhäuser, Berlin, 1993.

[KU87] A. N. Kolmogorov and V. A. Uspenskii. Algorithms and randomness. Translated in *Theory of Probability and its Applications*, 32:389–412, 1987.

[KW95] J. Köbler and O. Watanabe. New collapse consequences of NP having small circuits. In *Proceedings of the 22nd International Colloquium on Automata, Languages, and Programming*, pages 196–207. Springer-Verlag, 1995.

[Lau83] C. Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters*, 14:215–217, 1983.

[Lev73] L. A. Levin. On the notion of a random sequence. *Soviet Mathematics Doklady*, 14:1413–1416, 1973.

[LLS75] R. Ladner, N. Lynch, and A. Selman. A comparison of polynomial-time reducibilities. *Theoretical Computer Science*, 1:103–123, 1975.

[LM] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science.* To appear. See also *Proceedings of the Eleventh Symposium on Theoretical Aspects of Computer Science*, Springer–Verlag, 1994, pp. 415–426.

[LM94] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23:762–779, 1994.

[Luta] J. H. Lutz. Observations on measure and lowness for Δ_2^{P}. *Mathematical Systems Theory*. To appear. See also *Proceedings of the Thirteenth Symposium on Theoretical Aspects of Computer Science*, pages 87–97, Springer-Verlag, 1996.

[Lutb] J. H. Lutz. Resource-bounded measure. In preparation.

[Lut90] J. H. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19:1100–1131, 1990.

[Lut92] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.

[Lut95] J. H. Lutz. Weakly hard problems. *SIAM Journal on Computing*, 24:1170–1189, 1995.

[LV93] M. Li and P. M. B. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, 1993.

[LY90] L. Longpré and P. Young. Cook reducibility is faster than Karp reducibility in NP. *Journal of Computer and System Sciences*, 41:389–401, 1990.

[Lyn75] N. Lynch. On reducibility to complex or sparse sets. *Journal of the ACM*, 22:341–345, 1975.

[Mah82] S. R. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. *Journal of Computer and System Sciences*, 25:130–143, 1982.

[May94a] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136:487–506, 1994.

[May94b] E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 1994.

[May94c] E. Mayordomo. Measuring in PSPACE. In *Proceedings of the International Meeting of Young Computer Scientists '92*, pages 93–100. Gordon and Breach, 1994.

[Meh74] K. Mehlhorn. The "almost all" theory of subrecursive degrees is decidable. In *Proceedings of the Second Colloquium on Automata, Languages, and Programming*, pages 317–325. Springer Lecture Notes in Computer Science, vol. 14, 1974.

[Mey77] A. R. Meyer, 1977. Reported in [BH77].

[Nis92] N. Nisan. *Using Hard Problems to Create Pseudorandom Generators*. MIT Press, 1992.

[NW88] N. Nisan and A. Wigderson. Hardness vs. randomness. In *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, pages 2–11, 1988.

[OS86] P. Orponen and U. Schöning. The density and complexity of polynomial cores for intractable sets. *Information and Control*, 70:54–68, 1986.

[OW91] M. Ogiwara and O. Watanabe. On polynomial bounded truth-table reducibility of NP sets to sparse sets. *SIAM Journal on Computing*, 20(3):471–483, June 1991.

[Oxt80] J. C. Oxtoby. *Measure and Category*. Springer-Verlag, 1980. Second edition.

[Raz] A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izvestiya of the RAN*. To appear.

[RR94] A. Razborov and S. Rudich. Natural proofs. In *ACM Symposium on Theory of Computing*, pages 204–213, 1994.

[RS95] K. Regan and D. Sivakumar. Improved resource-bounded Borel-Cantelli and stochasticity theorems. Technical Report UB-CS-TR 95-08, Computer Science Department, University at Buffalo, 1995.

[RSC95] K. W. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. In *36th IEEE Symposium on Foundations of Computer Science*, pages 26–35. IEEE Computer Society Press, 1995.

[SC79] L. Stockmeyer and A. K. Chandra. Provably difficult combinatorial games. *SIAM Journal on Computing*, 8:151–174, 1979.

[Sch70] C. P. Schnorr. Klassifikation der Zufallsgesetze nach Komplexität und Ordnung. *Z. Wahrscheinlichkeitstheorie verw. Geb.*, 16:1–21, 1970.

[Sch71a] C. P. Schnorr. A unified approach to the definition of random sequences. *Mathematical Systems Theory*, 5:246–258, 1971.

[Sch71b] C. P. Schnorr. Zufälligkeit und Wahrscheinlichkeit. *Lecture Notes in Mathematics*, 218, 1971.

[Sch73] C. P. Schnorr. Process complexity and effective random tests. *Journal of Computer and System Sciences*, 7:376–388, 1973.

[Sch86a] U. Schöning. Complete sets and closeness to complexity classes. *Mathematical Systems Theory*, 19:29–41, 1986.

[Sch86b] U. Schöning. *Complexity and Structure*. Springer-Verlag, 1986.

[Sel79] A. L. Selman. P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP. *Mathematical Systems Theory*, 13:55–65, 1979.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[Sha49] C. E. Shannon. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28:59–98, 1949.

[Sip83] M. Sipser. A complexity-theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 330–335, 1983.

[Spe87] J. H. Spencer. *Ten Lectures on the Probabilistic Method*. SIAM, 1987.

[USS90] V. A. Uspenskii, A. L. Semenov, and A. Kh. Shen'. Can an individual sequence of zeros and ones be random? *Russian Mathematical Surveys*, 45:121–189, 1990.

[vM39] R. von Mises. *Probability, Statistics, and Truth*. Macmillan, 1939.

[Wat87a] O. Watanabe. A comparison of polynomial time completeness notions. *Theoretical Computer Science*, 54:249–265, 1987.

[Wat87b] O. Watanabe. *On the Structure of Intractable Complexity Classes*. PhD thesis, Tokyo Institute of Technology, 1987.

[Wil85] C. B. Wilson. Relativized circuit complexity. *Journal of Computer and System Sciences*, 31:169–181, 1985.

[WT92] O. Watanabe and S. Tang. On polynomial time Turing and many-one completeness in PSPACE. *Theoretical Computer Science*, 97:199–215, 1992.

[Yao82] A. Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, pages 80–91, 1982.

[You83] P. Young. Some structural properties of polynomial reducibilities and sets in NP. In *Proceedings of the Fifteenth ACM Symposium on Theory of Computing*, pages 392–401, 1983.